COORDINATED HIGHWAYS ACTION RESPONSE TEAM
STATE HIGHWAY ADMINISTRATION

CHART Release 13
Detailed Design
Rev 1

Contract SHA-06-CHART
Document # WO38-DS-001
Work Order 38, Deliverable 4

February 27, 2014
By
CSC

Revision	Description	Pages Affected	Date
0	Initial Release	All	01/03/2014
1	Changes to user interface section to show some modifications to the user list page.	4-3 through 4-5, with other figure number changes due to inserted figure.	02/27/2014

Table of Contents

Table of Figures

Table of Tables

1 Introduction

1.1 Purpose

This document describes the design of the software for CHART ATMS Release 13. The design for the corresponding R13 CHART Mapping update includes only an update to the Mapping ICD, which is not within the scope of this document. The CHART ATMS R13 release provides the following new features:

- **Security Policy Enhancements:** CHART ATMS R13 includes a number of enhancements to bring the ATMS into compliance with DoIT and MDOT Security requirements, particularly in the area of password management. These enhancements are briefly described below. They are all configurable.
    - The password minimum length, in accordance with current Security Policy, is configured as 8 for most users, and 11 for users designated as "System Administrators" within the CHART ATMS. Users will be designated as System Administrators if they are assigned a specific role which has been designated as the System Administrator role within the CHART ATMS.
    - A password must contain certain (configurable) minimum numbers of characters of various classes, such as letters (uppercase, lowercase, or any case), digits, and special characters. A space is a valid character in a password, as long as it is not at the beginning or end of the password.
    - Passwords are checked against a dictionary of English words and proper names.
    - Passwords cannot contain excessive (configurable) numbers of characters "in sequence", as defined by configurable sequence strings (such as "abcdef…", "1234…", "qwerty..." etc.)
    - Passwords cannot contain excessive (configurable) numbers of the same character (for instance, "a1a1a1a1" could be considered invalid by this rule).
    - Passwords expire after a certain (configurable) number of days. The expiration time varies depending on whether the user is classified as an ATMS System Administrator or not. 2013 Security Policy demands 30 days for System Administrators and 45 days for other users. If a user logs in with an expired password, the user must immediately change the password before the system can be accessed. Users are also required to change their password upon their first login after an administrator has set or reset their password.
    - A user cannot reuse any of the last configurable number of most recently used passwords. Current Security Policy demands 10 most recently used passwords be maintained. (These passwords, as always, will be stored in encrypted form only.) Also, passwords cannot be changed too frequently in order to circumvent this rule (current policy prohibits more than one change every two days).

  - A user cannot change his/her password only by adding, changing, or deleting a single character in the password.
  - User accounts can be disabled without completely deleting them, for instance if a user goes on vacation; also, the system will automatically disable accounts not used for a certain (configurable) period of time (current policy demands 60 days). ATMS administrators can easily see enabled or disabled accounts, and can enable or disable user accounts at any time.
  - A user account will be automatically locked for a (configurable) period of time after a repeated number of consecutive failed login attempts. (This is not the same as "disabling" an account – no administrator involvement is required to unlock the account.)
  - The ATMS will provide a warning to the user prior to the user logging in, advising that access is restricted to authorized users only, that unauthorized use is prohibited and subject to prosecution, that user activity on the system is monitored, that data created becomes property of the State of Maryland, etc.
  - After the user is logged in, the time of the most recent successful login and most recent successful logout will be displayed to the user. (The hope is that a user might notice a login/logout that he/she did not initiate.)
- **FITM Plans:** CHART ATMS R13 provides users with the ability to view Freeway Incident Traffic Management (FITM) Plans. FITM Plans are pre-defined detour plans used to divert traffic around road closures or for other special events such as evacuation. FITM plans include detour maps which are depicted in files having Adobe PDF file format, and they are also attributed with other metadata describing their location. There are currently at least 400 FITM plans defined.

  - CHART ATMS R13 allows users of the CHART ATMS GUI to view the FITM plans defined in the system. In the main usage scenario, a user opens a traffic event and wishes to view the FITM plans near that event. (Typically only the FITM plans "upstream" from the event are useful, as traffic must be diverted upstream from a road closure; however, because it can be problematic for the system to determine which may be "upstream", R13 uses a search based on a configurable radius and thresholds for the minimum / maximum number of "nearby" plans to display.) R13 displays a list of nearby FITM plans by default, but if the desired plan is not in the list, the user can also view the list of All FITM Plans (which is initially hidden if there are nearby FITM plans). If a user views a FITM plan from the context of a traffic event, a log entry is added to the event history log.

  - R13 also allows the user to view the list of FITM plans from the ATMS GUI main menu (i.e., outside the context of a traffic event). This may be useful for viewing regional evacuation plans, or just for browsing purposes. A new functional right is added in R13 to control access to this feature.

- **COTS Upgrades:** CHART ATMS R13 includes several COTS upgrades. These upgrades provide no visible changes for ATMS users; they are intended only to bring the ATMS up to date with these products. The products being updated, and their new versions, are:
  - Java 7u45
  - Apache Tomcat 7.0.47
  - JavaScript library prototype.js 1.7.1
  - OpenLayers 2.13.1
  - Microsoft Visual Studio 2012
  - Apache Flex 4.6

1.2 Objectives

The main objective of this detailed design document is to provide software developers with a framework in which to implement the requirements identified in the CHART ATMS R13 Requirements document. A matrix mapping requirements to the design is presented in Section 7 (Mapping to Requirements).

1.3 Scope

This design is limited to Release 13 of the CHART ATMS. It addresses both the design of the server components of CHART ATMS and the Graphical User Interface (GUI) components of CHART ATMS to support the new features being added. This design does not include designs for components implemented in earlier releases of the CHART ATMS.

1.4 Design Process

The design was created by capturing the requirements of the system in UML Use Case diagrams. Class diagrams were generated showing the high level objects that address the Use Cases. Sequence diagrams were generated to show how each piece of major functionality will be achieved. This process was iterative in nature – the creation of sequence diagrams sometimes caused re-engineering of the class diagrams, and vice versa.

1.5 Design Tools

The work products contained within this design were extracted from the Enterprise Architect design tool. Within this tool, the design is contained in the project named “chartdesign” in the folder named “CHART-ATMS-R13”.

1.6 Work Products

The final CHART ATMS Release 13 design consists of the following work products:

- Human-Machine Interface section which provides descriptions of the screens that are changing or being added in order to allow the user to perform the described uses.
- Use Case diagrams that capture the requirements of the system

- UML Class diagrams, showing the software objects which allow the system to accommodate the uses of the system described in the Use Case diagrams
- UML Sequence diagrams showing how the classes interact to accomplish major functions of the system
- Requirement Verification Traceability Matrix that shows how this design meets the documented requirements for this feature

2 Architecture

The sections below discuss specific elements of the architecture and software components that are created, changed, or used in CHART ATMS Release 13.

2.1 Network/Hardware

CHART ATMS Release 13 features do not impact the network or hardware architecture of the CHART system.

2.2 Software

CHART ATMS uses the Common Object Request Broker Architecture (CORBA) as the base architecture, with custom built software objects made available on the network allowing their data to be accessed via well defined CORBA interfaces. Communications to remote devices use the Field Management Server (FMS) architecture. Newer external interfaces such as the User Management web service, Data Exporter, and GIS service employ a web services architecture combining an HTTP request/response structure to pass XML messages.

Except where noted in the subsections below, CHART ATMS Release 13 features do not impact the software architecture of the CHART ATMS.

2.2.1 COTS Products

2.2.1.1 CHART ATMS

CHART ATMS uses numerous COTS products for both run-time and development. No additional COTS products are added as part of R13. Table 2-1 contains existing COTS products. Some of these are changed for CHART ATMS Release 13, and these are noted in bold.

Table 2-1. ATMS COTS Products

Product Name	Description
Adobe Flex SDK	**CHART R13 uses the Flex SDK 4.6 to provide the Flex compiler, the standard Flex libraries, and examples for building Flex applications used by the CHART ATMS GUI. (CHART R12 used Flex SDK 3.3)**
Apache ActiveMQ	CHART uses this to connect to RITIS JMS queues.
Apache Jakarta Ant	CHART uses Apache Jakarta Ant 1.6.5 to build CHART applications and deployment jars.
Apache Tomcat	**CHART R13 uses Apache Tomcat 7.0.47 as the GUI web server. (CHART R12 used 6.0.29).**
Apache XML-RPC	CHART uses the apache xmlrpc java library 3.1.2 protocol that uses XML over HTTP to implement remote procedure calls. The video Flash streaming “red button” (“kill switch”) API uses XML over HTTP remote procedure calls.
Bison/Flex	CHART uses Bison and Flex as part of the process of compiling binary macro files used for performing camera menu operations on Vicon Surveyor VFT cameras.
bsn.autosuggest	The event resource search feature and the EORS integration feature use version 2.1.3 of the bsn.autosuggest JavaScript code from brandspankingnew.net. This tool is freely available and is included as source code in the CHART GUI. It provides a simple JavaScript tool that can be associated with a text entry field. It uses AJAX

Product Name	Description
	to provide search results / suggestions as the user types.
CoreTec Decoder Control	CHART uses a CoreTec supplied decoder control API for commanding CoreTec decoders.
Dialogic API	CHART uses the Dialogic API for sending and receiving Dual Tone Multi Frequency (DTMF) tones for HAR communications.
GIF89 Encoder	Utility classes that can create .gif files with optional animation. This utility is used for the creation of DMS True Display windows.
JAXB	CHART uses the jaxb java library to automate the tedious task of hand-coding field-by-field XML translation and validation for exported data.
JDOM	CHART uses JDOM b7 (beta-7) dated 2001-07-07. JDOM provides a way to represent an XML document for easy and efficient reading, manipulation, and writing.
JacORB	CHART uses a compiled, patched version of JacORB 2.3.1. The JacORB source code, including the patched code, is kept in the CHART source repository.
JavaMail API	The CHART Notification Service uses the JavaMail API 1.4.4, an optional Java package which provides SMTP e-mail support.
Java Run-Time (JRE)	**CHART R13 uses 1.7.0_45. (CHART R12 used 1.7.0_07)**
JavaService	CHART uses JavaService to install the server side Java software components as Windows services.
JAXEN	CHART uses JAXEN 1.0-beta-8 dated 2002-01-09. The Jaxen project is a Java XPath Engine. Jaxen is a universal object model walker, capable of evaluating XPath expressions across multiple models.
JoeSNMP	CHART uses JoeSNMP version 0.2.6 dated 2001-11-11. JoeSNMP is a Java based implementation of the SNMP protocol. CHART uses for commanding iMPath MPEG-2 decoders and for communications with NTCIP DMSs.
JSON-simple	CHART uses the JSON-simple java library to encode/decode strings that use JSON (JavaScript Object Notation).
JTS	CHART uses the Java Topology Suite (JTS) version 1.8.0 for geographical utility classes.
Log4J	CHART uses the log4J version 1.2.15 for logging purposes.
Microsoft Visual Studio	**CHART R13 uses Visual Studio 2012 to build native JNI DLLs and executables. (CHART R12 used Visual Studio 2010).**
NSIS	CHART uses the Nullsoft Scriptable Installation System (NSIS), version 2.45, as the server side installation package.
NeoSpeech Text To Speech	For text-to-speech (TTS) conversion CHART uses NeoSpeech TTS version 3.10.7.
OpenLayers	**CHART R13 ATMS GUI uses the OpenLayers JavaScript API 2.13.1 (http://openlayers.org/) in order to render interactive maps without relying on vendor specific software. OpenLayers is an open source product released under a BSD style license which can be found at (http://svn.openlayers.org/trunk/openlayers/license.txt). (CHART R12 used OpenLayers 2.11)**
O'Reilly Servlet	Provides classes that allow the CHART GUI to handle file uploads via multi-part form submission.
Prototype Javascript Library	**The CHART R13 ATMS GUI uses the Prototype JavaScript library, version 1.7.1, a cross-browser compatible JavaScript library provides many features (including easy Ajax support). (CHART R12 used version Prototype 1.7)**
SAXPath	CHART uses SAXPath 1.0-beta-6 dated 2001-09-27. SAXPath is an event-based API for XPath parsers, that is, for parsers which parse XPath expressions.
MSSQL Server	CHART uses MS SQLServer (2008 R2) as its database and uses the MS SQL Server JDBC libraries (sqljdbc4.jar) for all database transactions.
SQLServer JDBC Driver	CHART uses this driver to lookup GIS related data and also to store Location

Product Name	Description
	Aliases in SQL Server databases.
Velocity Template Engine	Provides classes that CHART GUI uses in order to create dynamic web pages using velocity templates, CHART uses Velocity version 1.6.1 and tools version 1.4.
Vicon V1500 API	CHART uses a Vicon supplied API for commanding the ViconV1500 CPU to switch video on the Vicon V1500 switch.

2.2.2 Deployment /Interface Compatibility

2.2.2.1 CHART ATMS

2.2.2.1.1 External Interfaces

This section describes the external interfaces being added in Release 13 of CHART ATMS. See Figure 2-1.

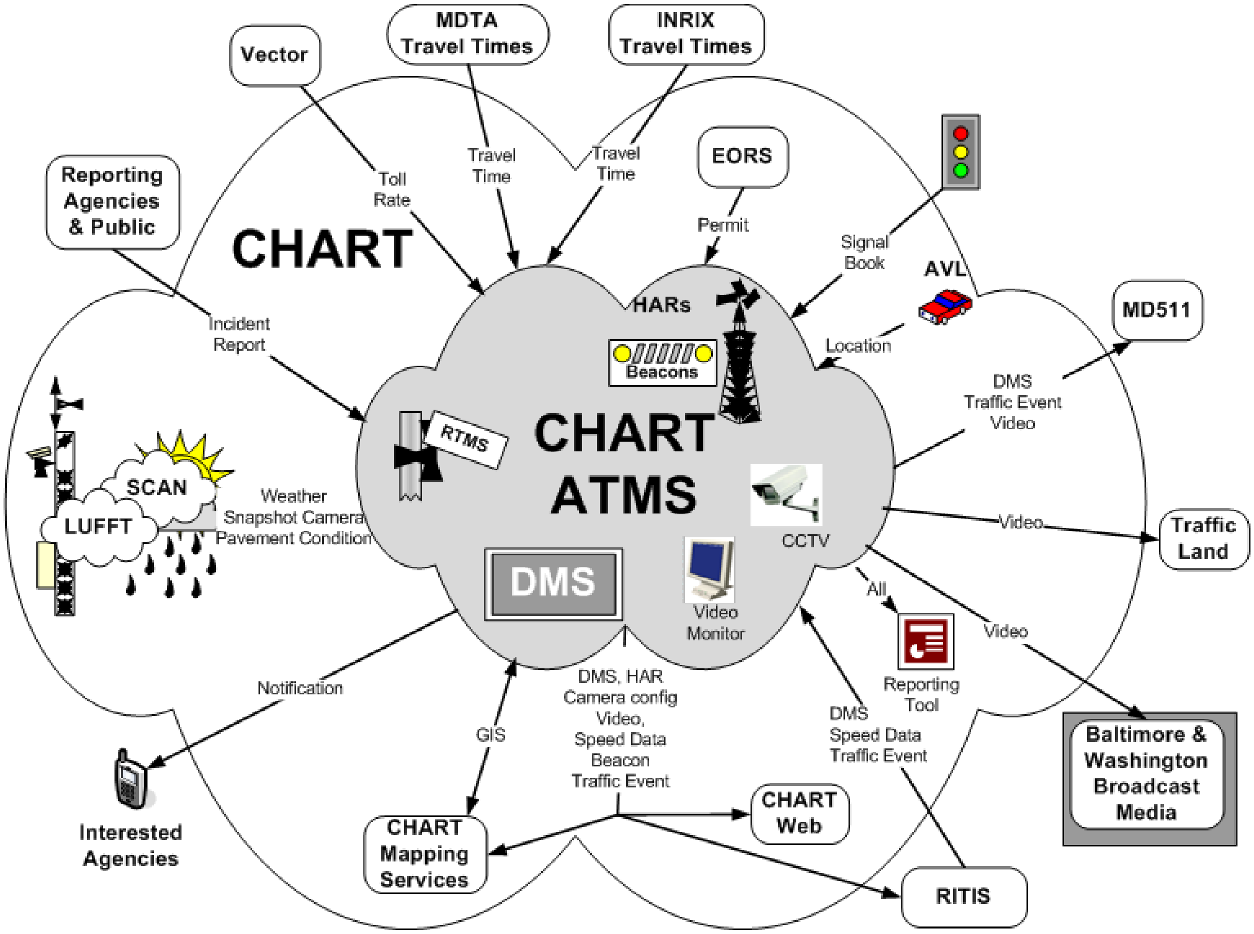


Figure 2-1. CHART and External Interfaces

No external interfaces are modified or added for R13.

Server and GUI deployment diagrams are shown in Figure 2-2 and Figure 2-3. The CHART ATMS GUI deployment diagram is changed in R13 to show the GUI interface to the new FITM mapping web service.

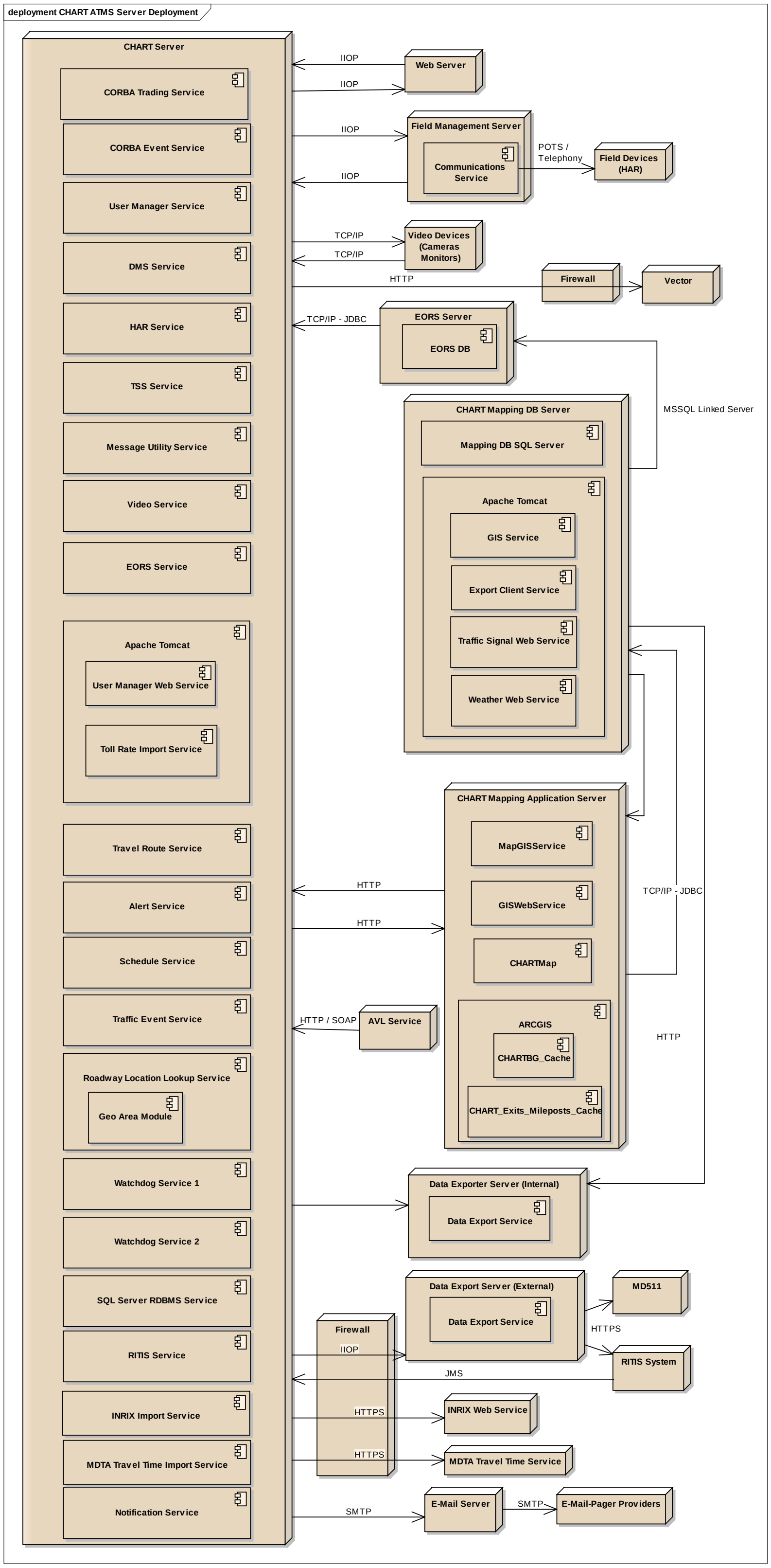


Figure 2-2. R13 Server Deployment

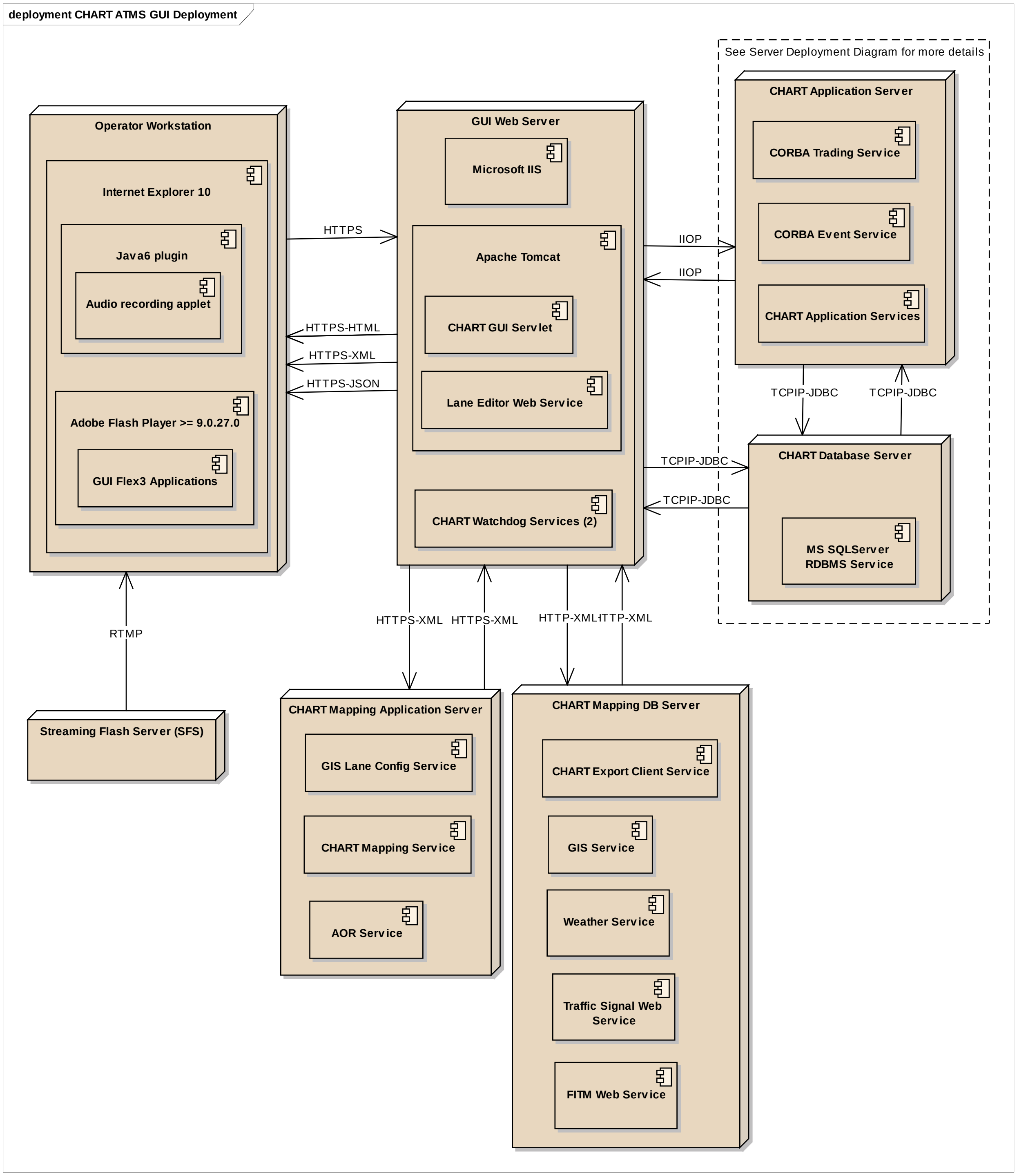


Figure 2-3. R13 GUI Deployment

2.2.2.1.2 Internal Interfaces

This section describes the internal interfaces being added or modified in Release 13 of the CHART system.

The R13 Security Policy Enhancements feature requires modification to several existing CORBA interfaces and structures. A user account is now marked as a normal account or System Administrator account (for setting password rules for the account); can now be disabled (automatically due to non-use or manually) or enabled (manually); and can be locked (automatically due to excessive failed login attempts) or unlocked (automatically after a brief lockout period); therefore user information will now contain an admin flag, a disabled flag and an unlock timestamp. A user account can be created in the disabled state, so a disabled flag is also passed in as an account is created. A user can be forced to change his/her password (due to password expiration or if the current password was administratively set/reset), so the user information also contains a flag indicating the password must be changed. This flag is passed back to the GUI upon successful login, along with the most recent previous successful login and logout times, which are displayed to the user upon login.

2.3 Security

This section describes the security being added or modified in Release 13 of CHART ATMS. The Security Policy Enhancements feature of R13 is aimed directly at security. See Section 1.1 for the security features added in R13.

2.4 Data

CHART ATMS Release 13 will be tested and delivered with the fielded MS SQL Server version.

2.4.1 Data Storage

The CHART ATMS stores most of its data in a non-spatial MS SQL Server database. Additionally the Integrated Map feature adds the ability to store location aliases to the spatial SQL Server database. Some data is stored in flat files on the CHART servers.

This section describes all of these types of data.

2.4.1.1 Database

2.4.1.1.1 Database Architecture

Except as noted, CHART ATMS Release 13 features do not impact the overall architecture of the CHART ATMS database.

2.4.1.1.2 Logical Design

2.4.1.1.2.1 CHART Entity Relationship Diagram (ERD)

CHART ATMS Database entity relationship diagram for R13 is shown below in the fifteen figures which follow, Figure 2-3 through Figure 2-17. These figures should be mentally arranged into a grid five images wide and three images tall, if desired to follow the connector lines which go off the pages. Pages 2-1 through 5-1 are to the right of Page 1-1, and Pages 1-2 and 1-3 are below Page 1-1. For instance, the connector lines which come out the bottom of Page 2-1 (Figure 2-4) come into the top of Page 2-2 (Figure 2-9). The Table Definition Report sections that follow describe the changes that will be made for R13. The changes for R13 are isolated to Figure 2-5.

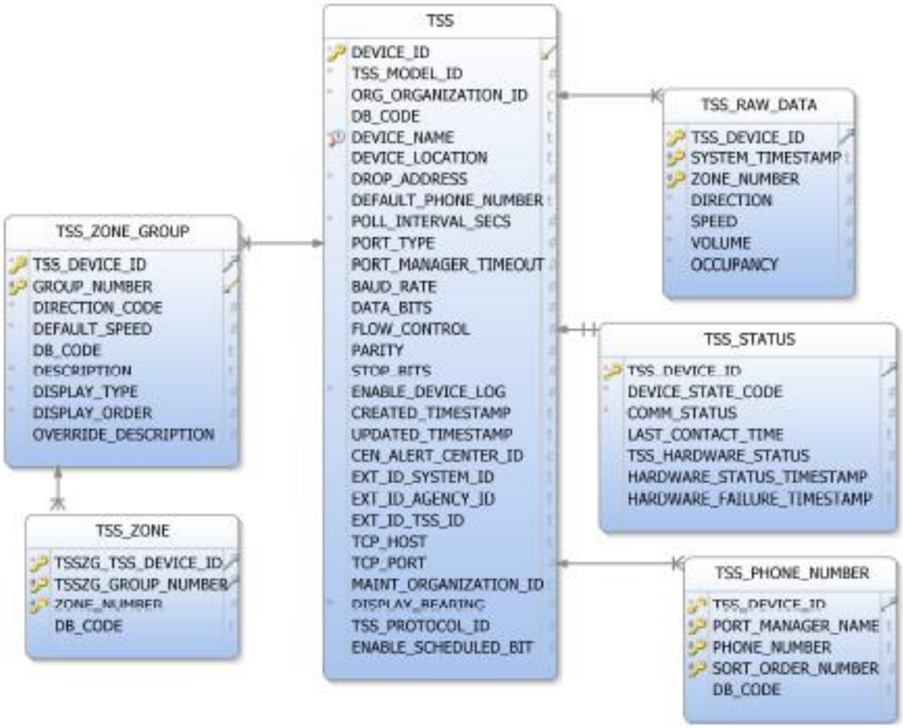


Figure 2-4. CHART_Live ERD, Page 1-1

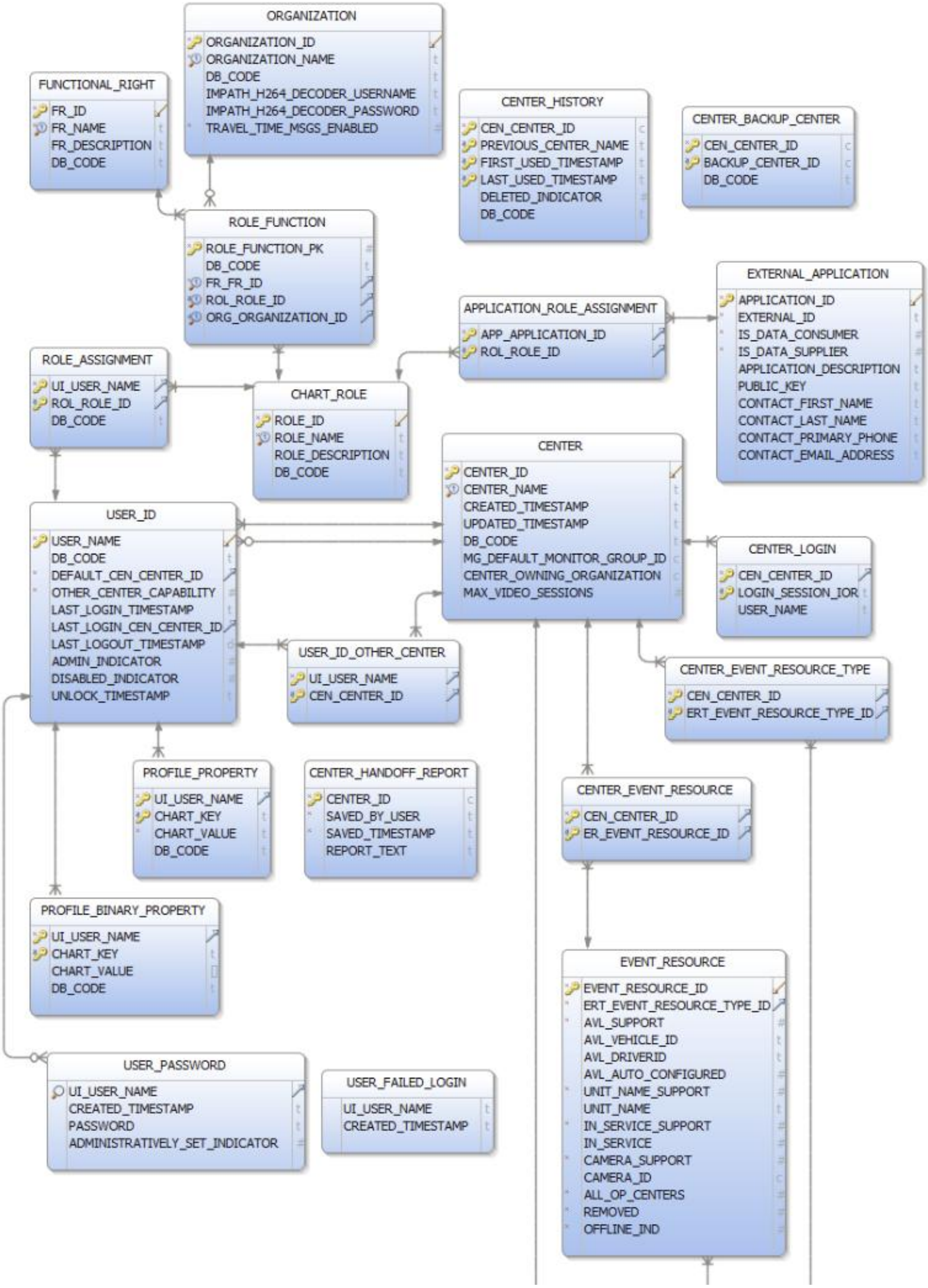


Figure 2-5. CHART_Live ERD, Page 2-1

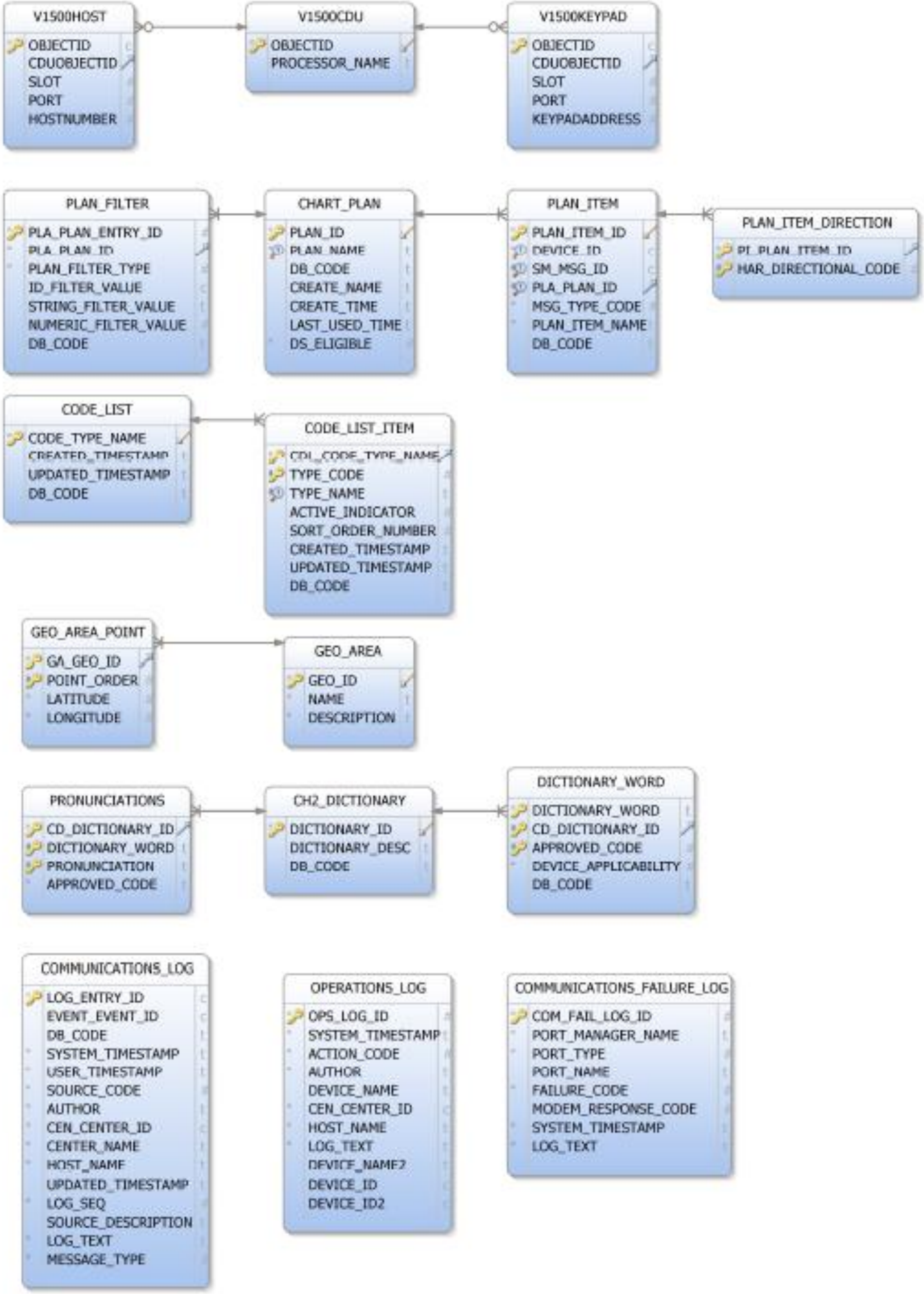


Figure 2-6. CHART_Live ERD, Page 3-1

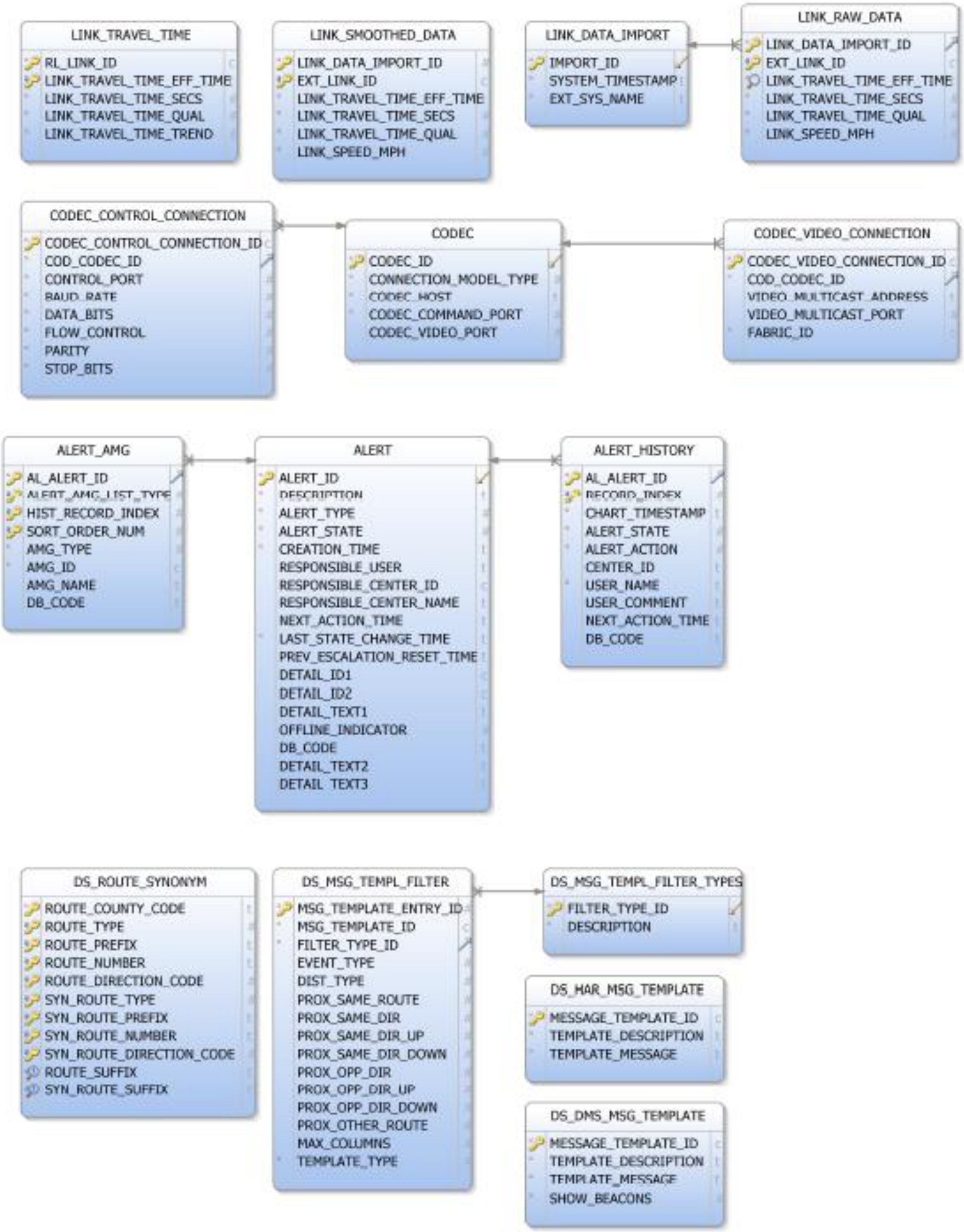


Figure 2-7. CHART_Live ERD, Page 4-1

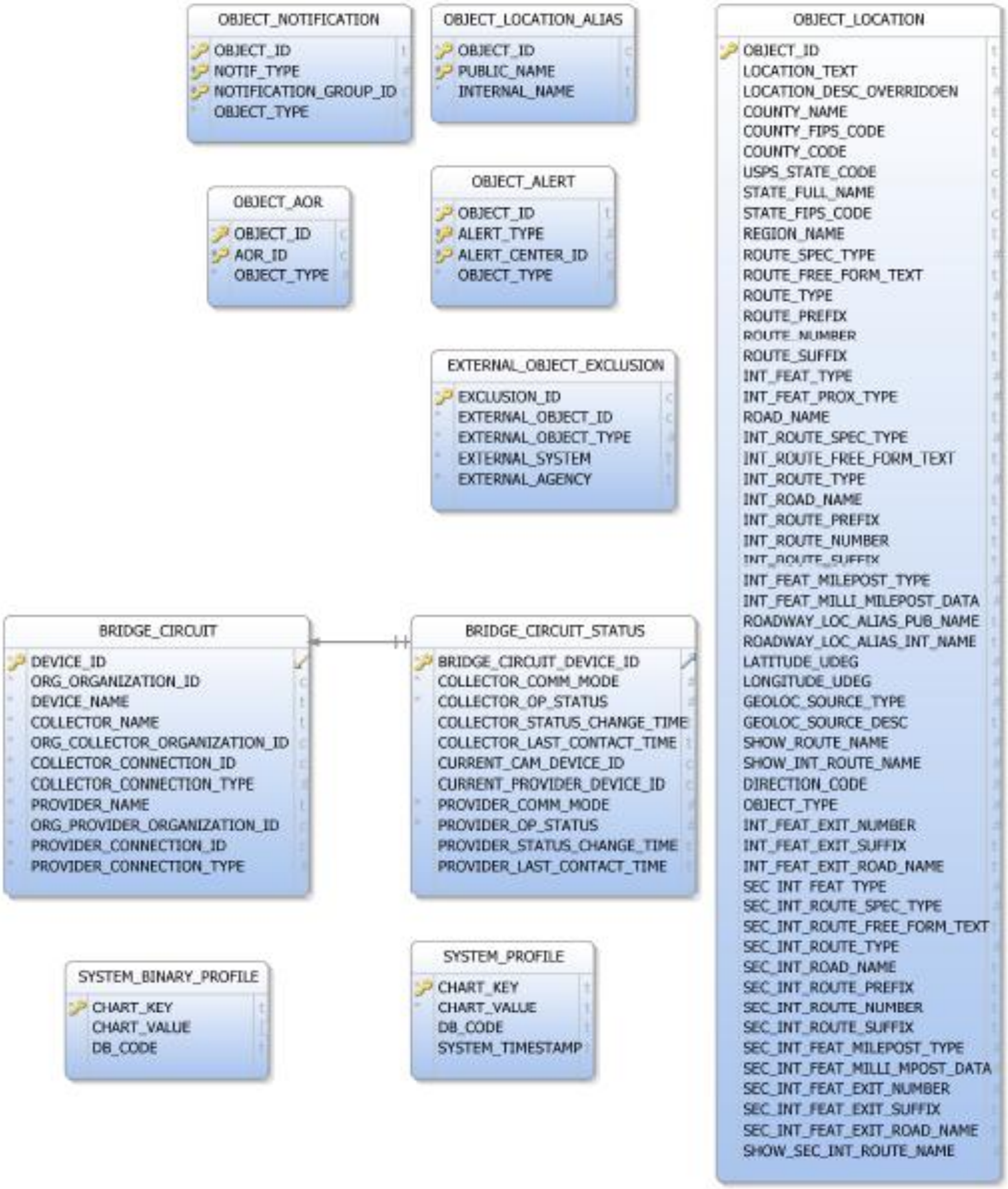


Figure 2-8. CHART_Live ERD, Page 5-1

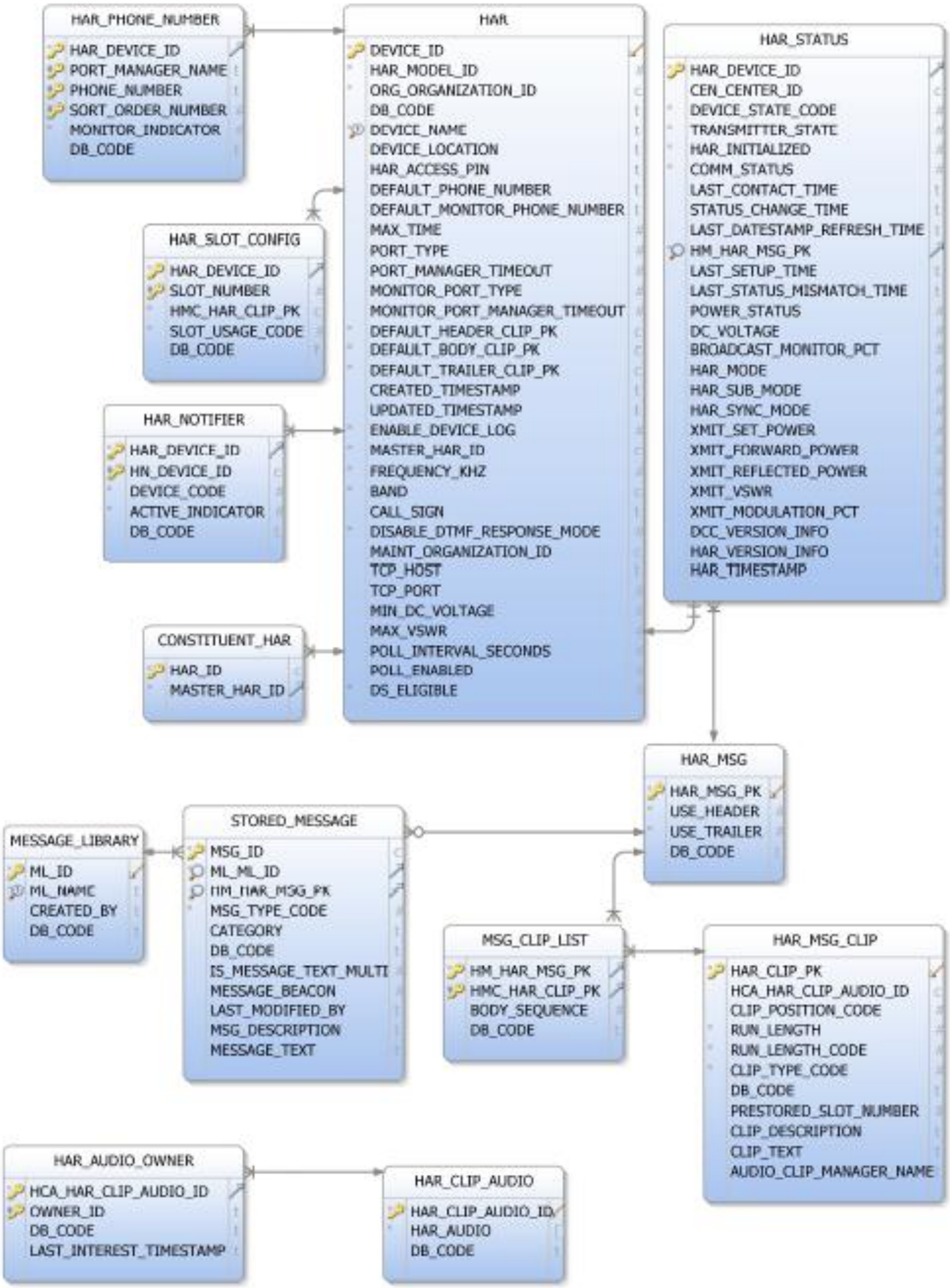


Figure 2-9. CHART_Live ERD, Page 1-2

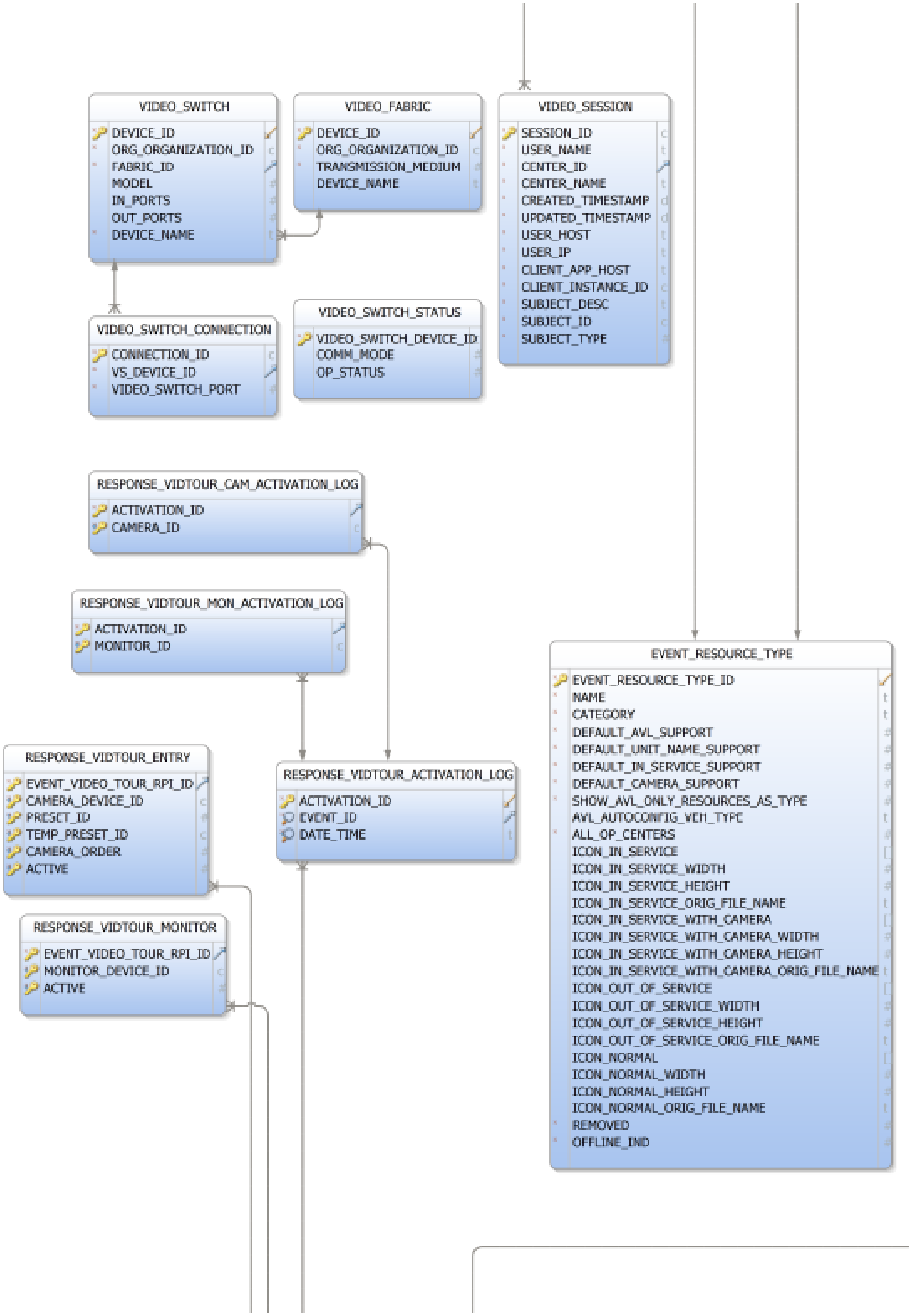


Figure 2-10. CHART_Live ERD, Page 2-2

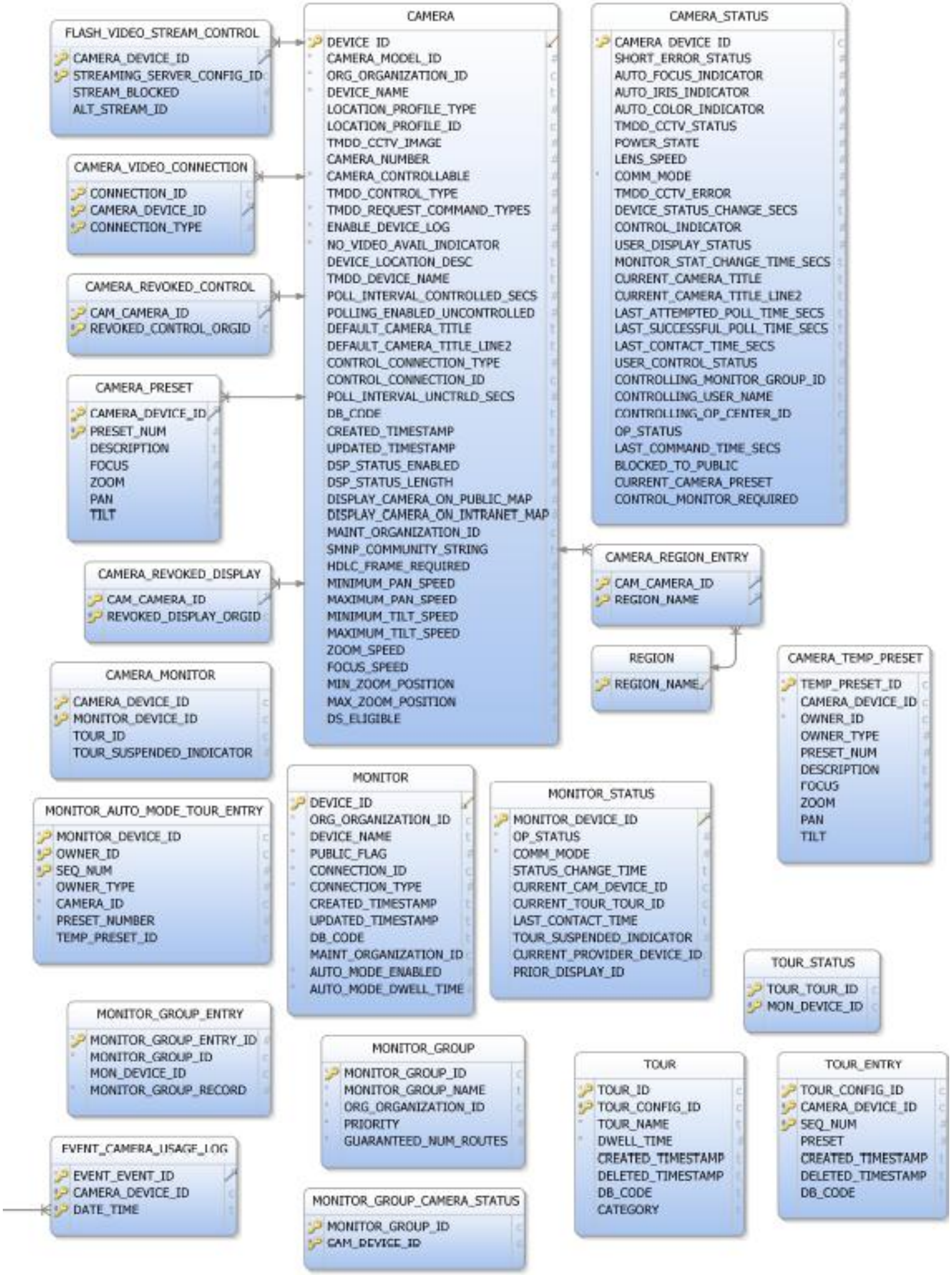


Figure 2-11. CHART_Live ERD, Page 3-2

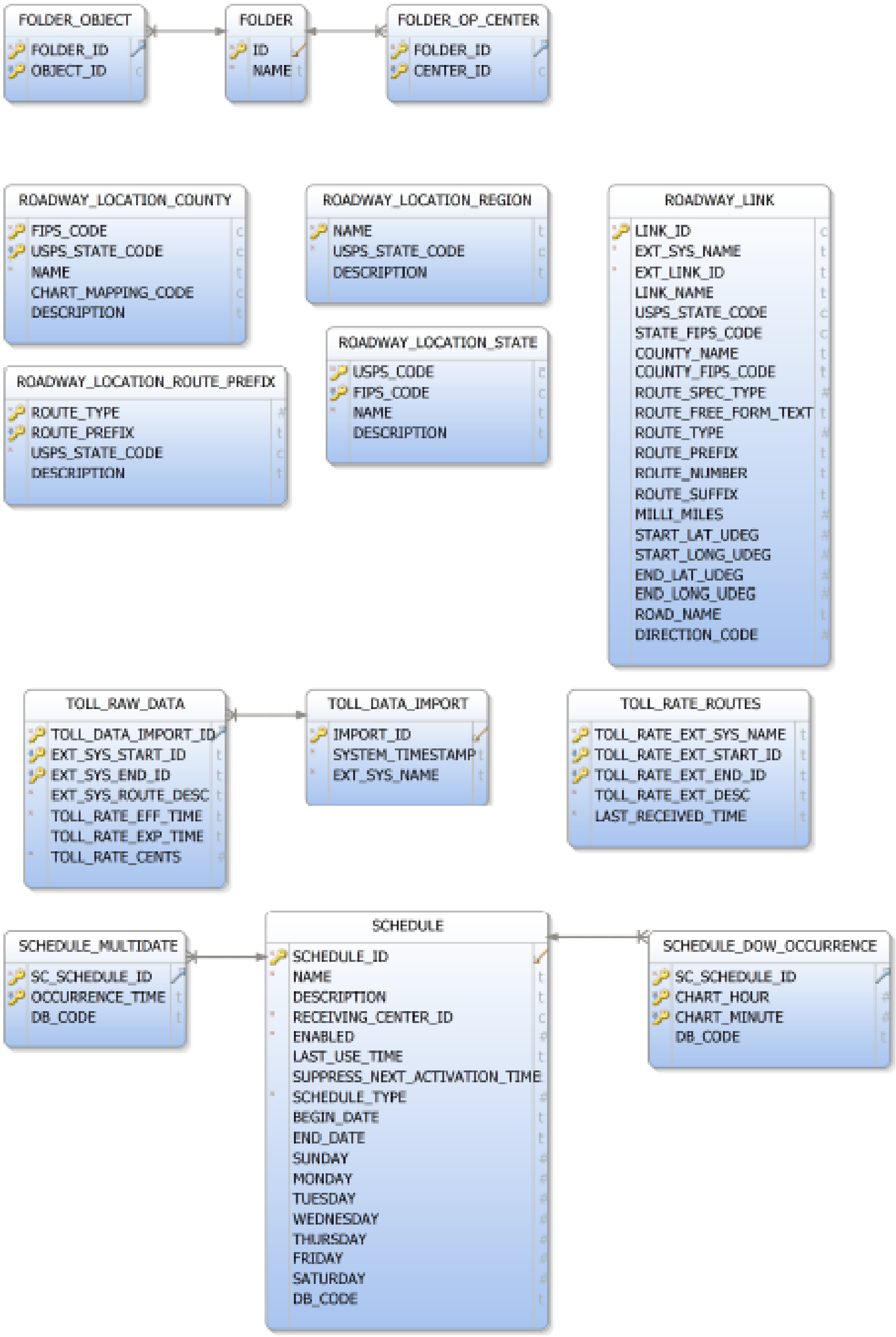


Figure 2-12. CHART_Live ERD, Page 4-2

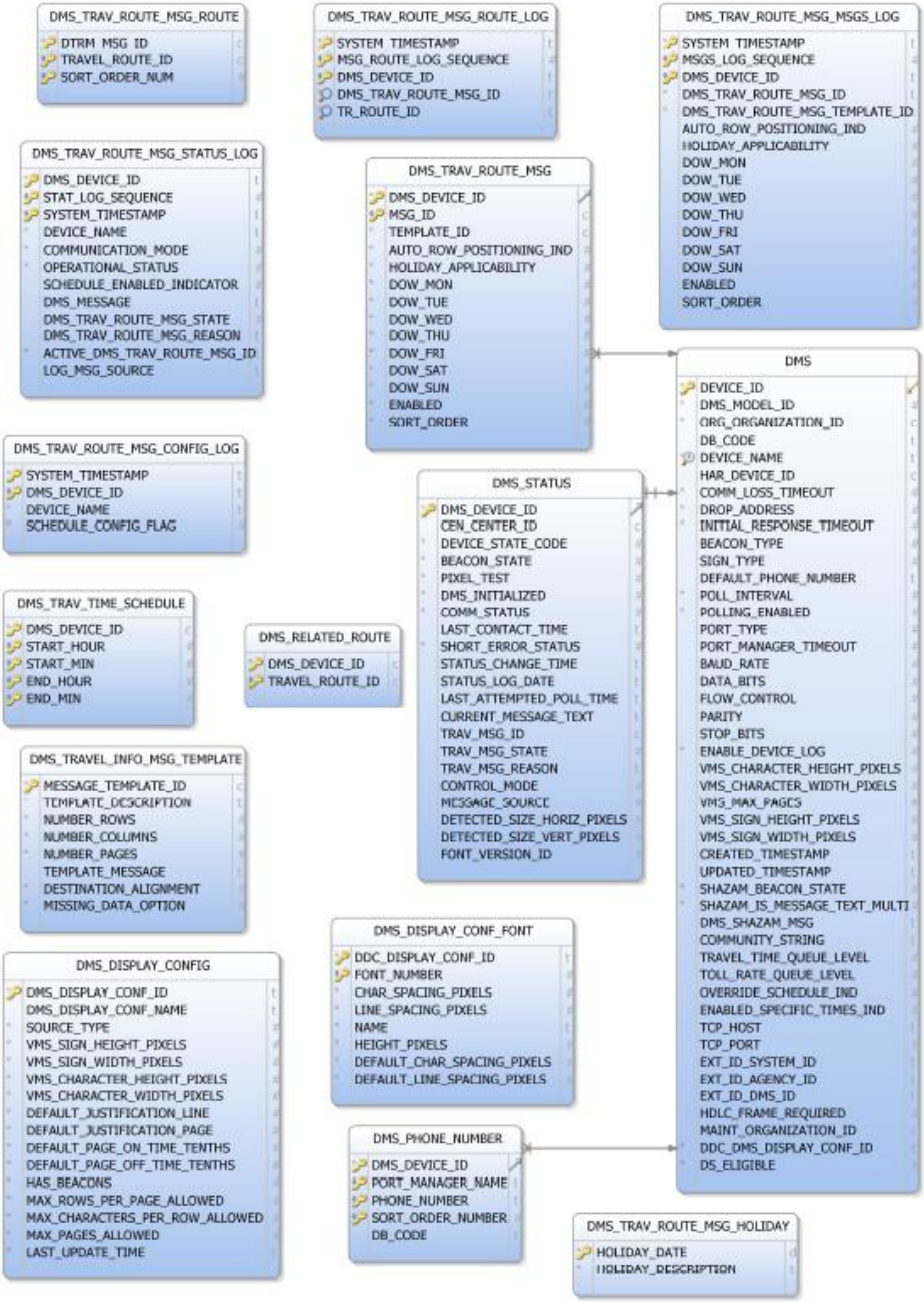


Figure 2-13. CHART_Live ERD, Page 5-2

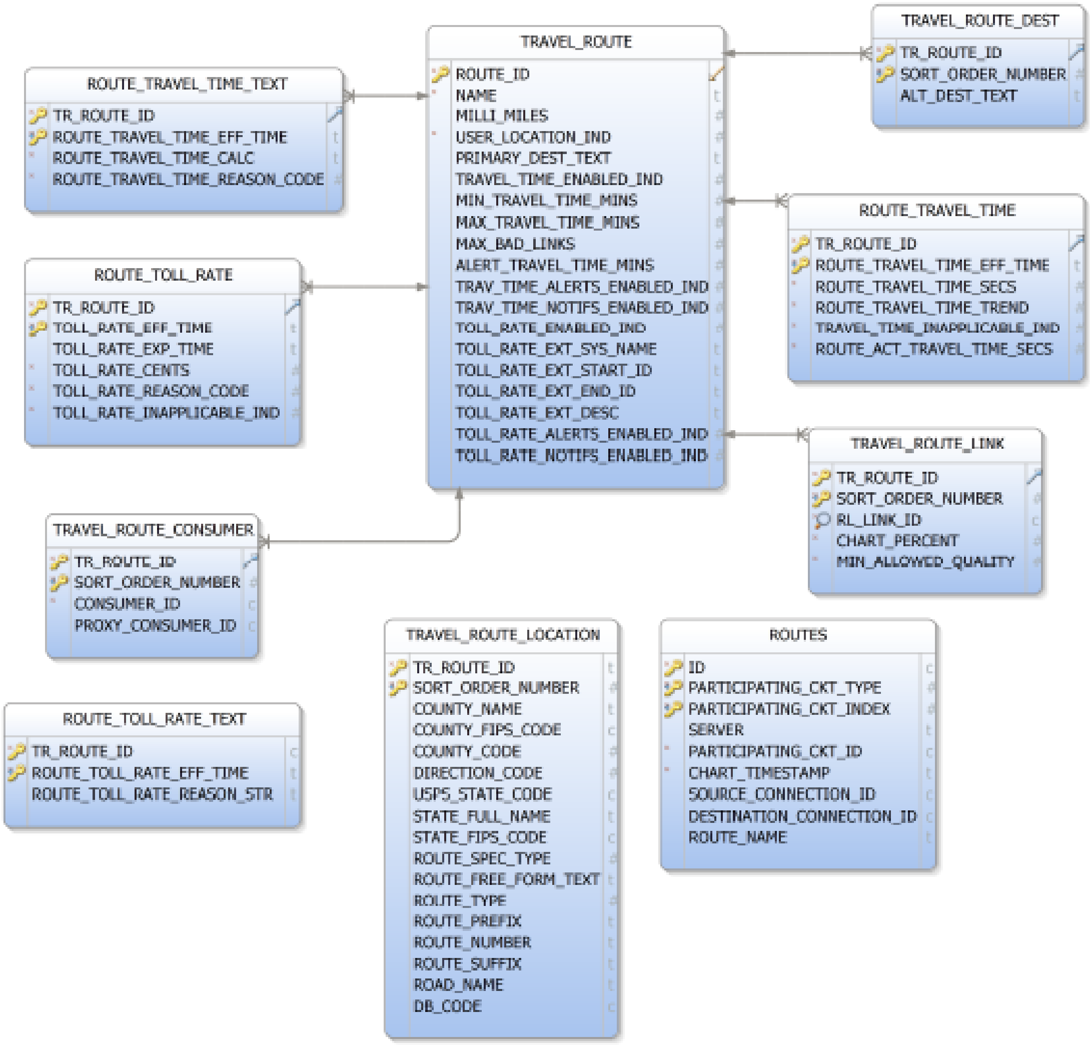


Figure 2-14. CHART_Live ERD, Page 1-3

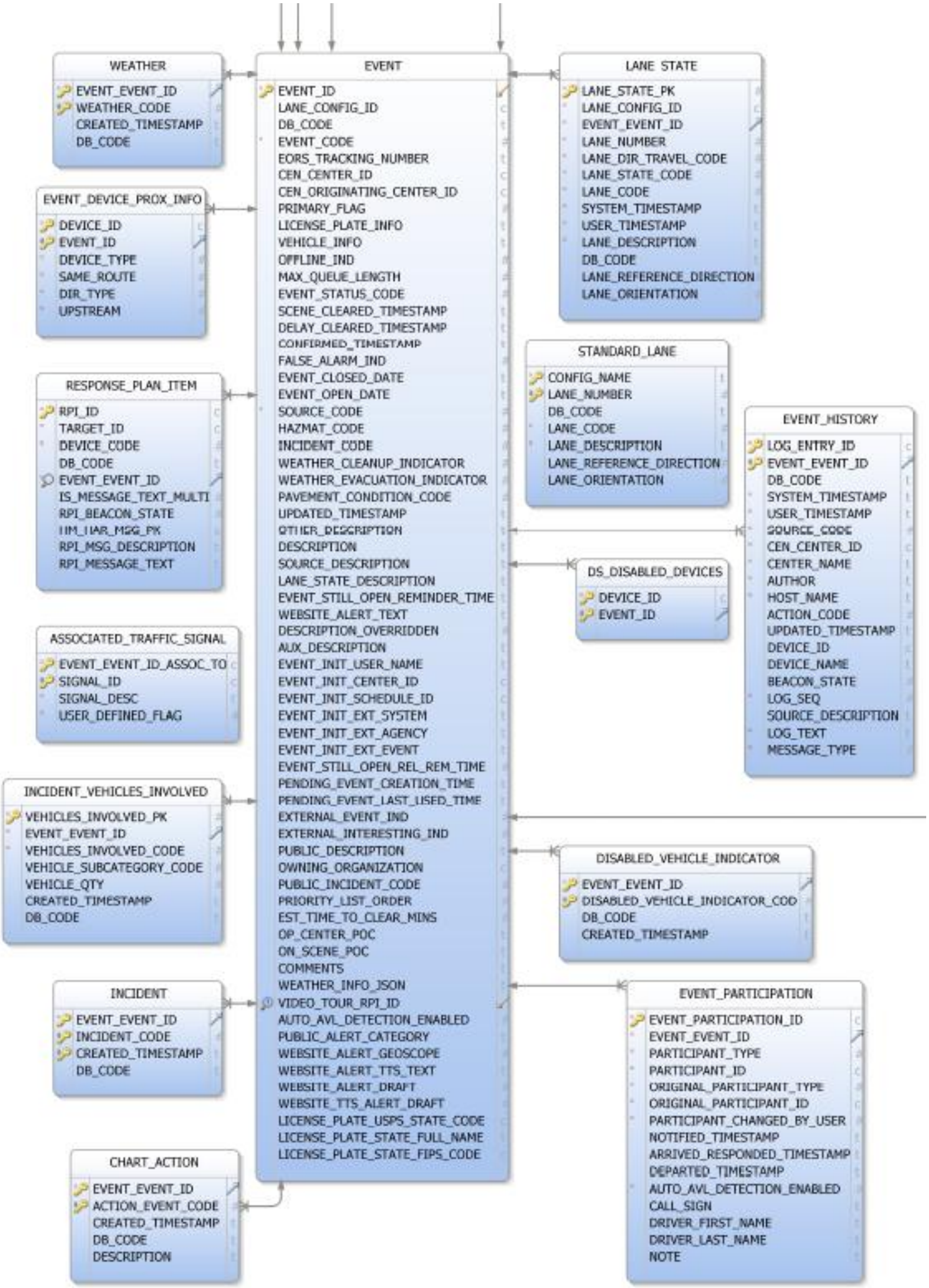


Figure 2-14. CHART_Live ERD, Page 2-3

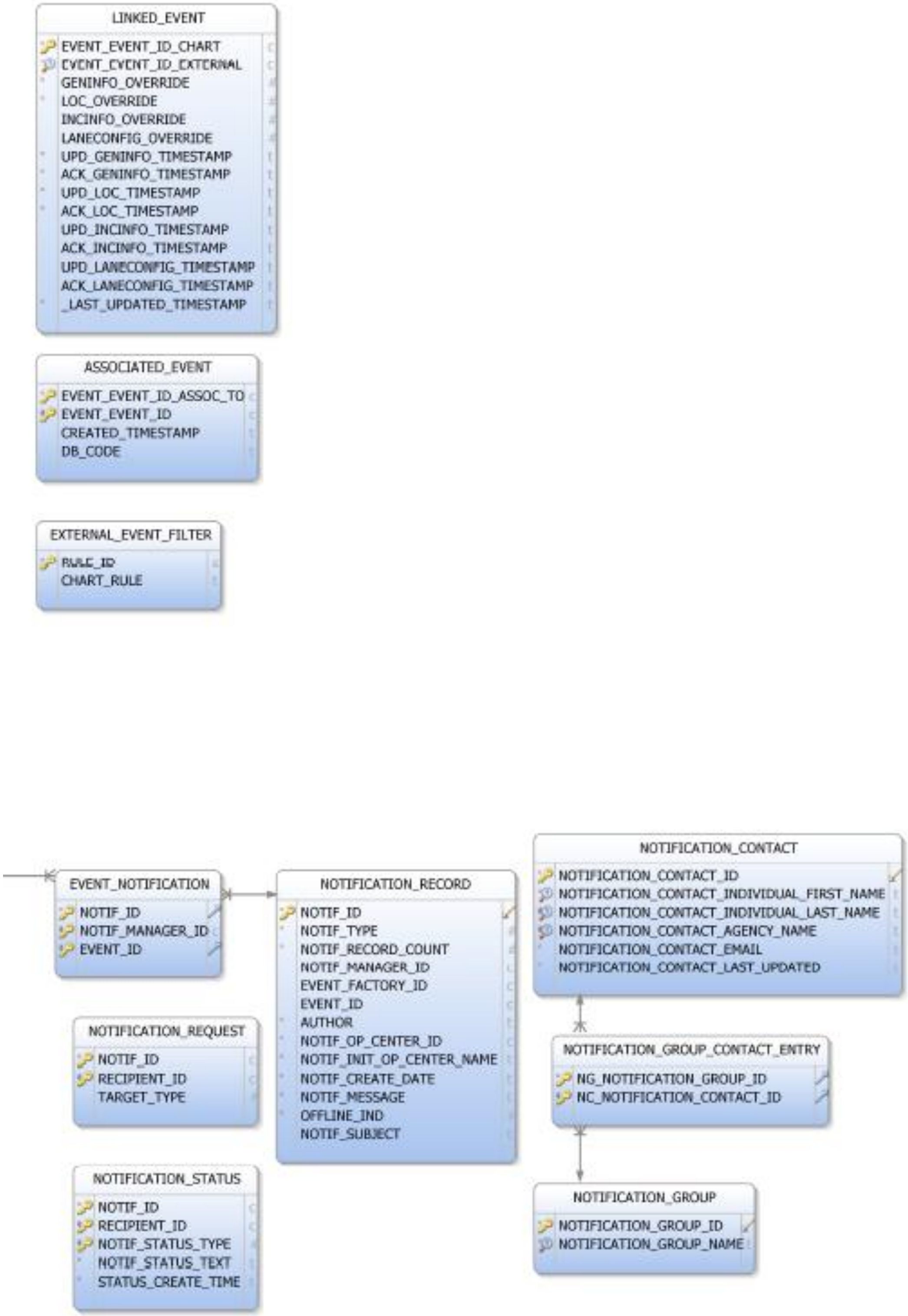


Figure 2-15. CHART_Live ERD, Page 3-3

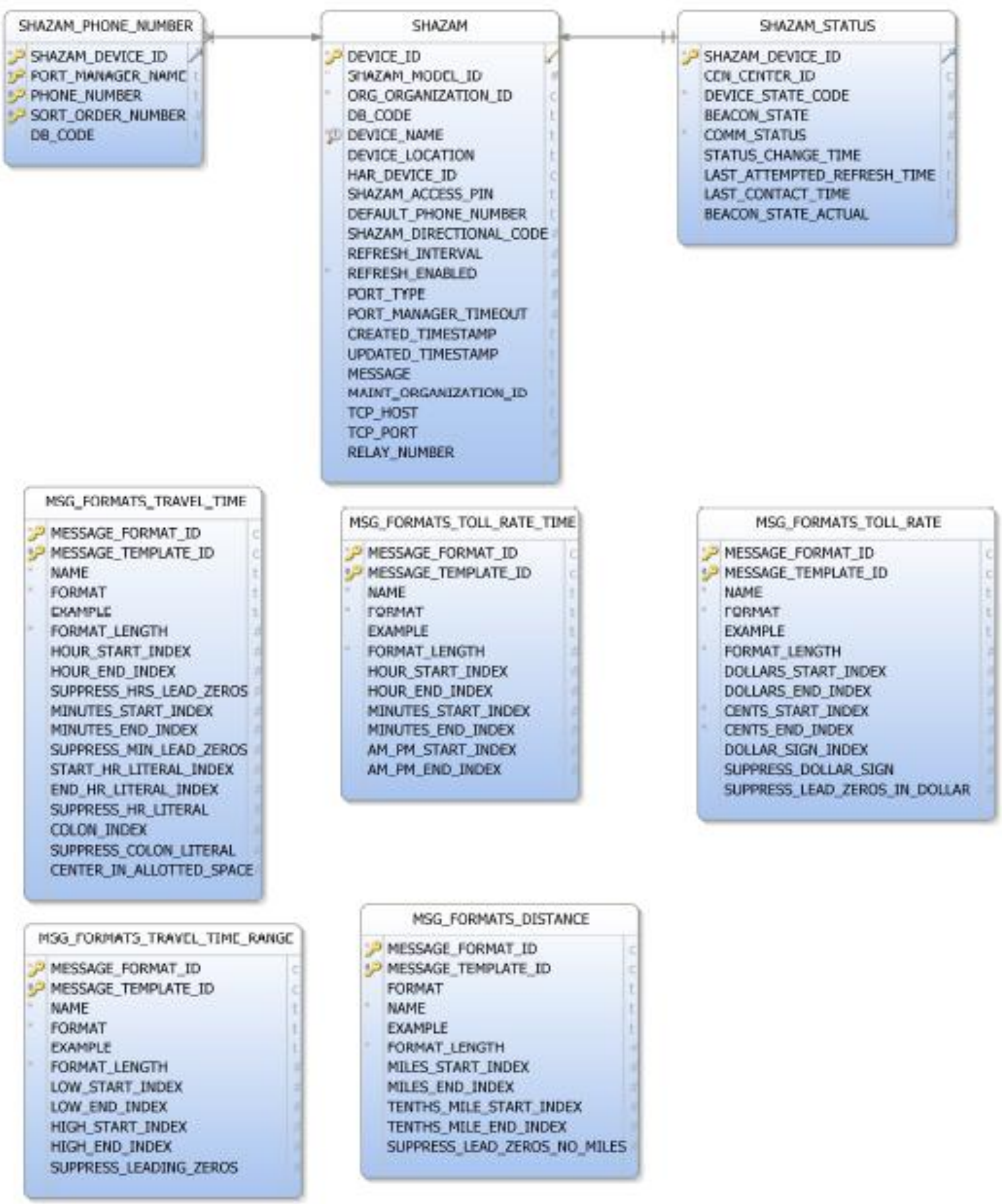


Figure 2-16. CHART_Live ERD, Page 4-3

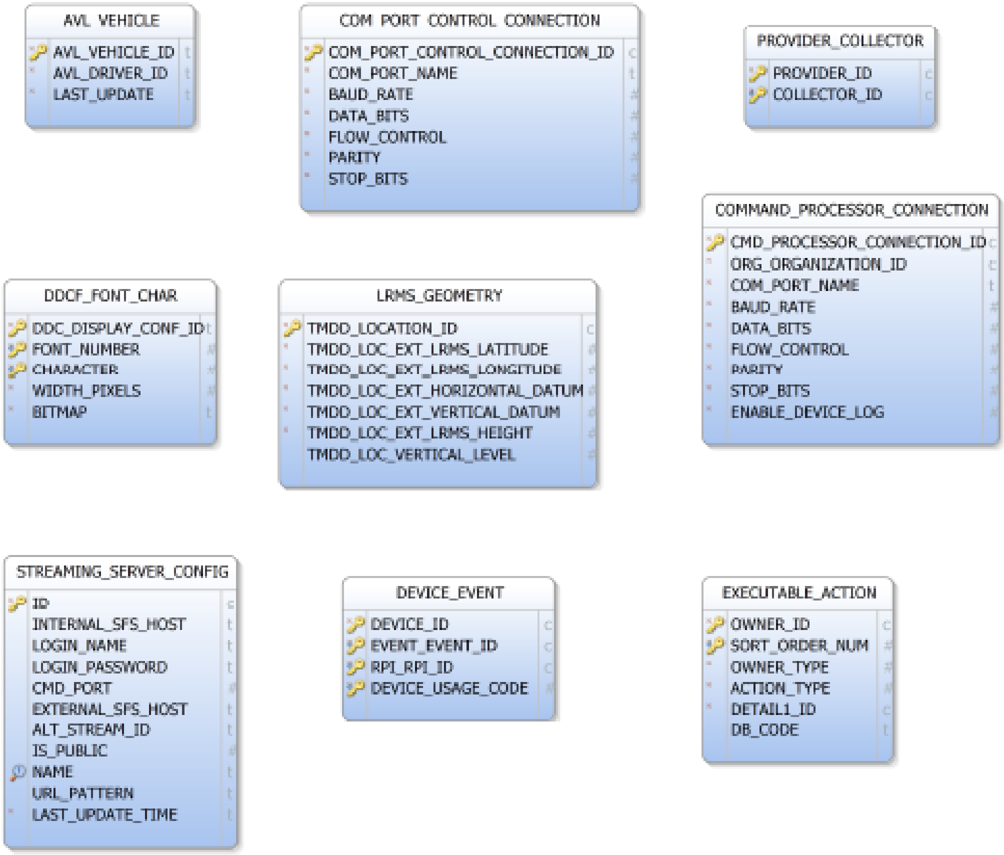


Figure 2-17. CHART_Live ERD, Page 5-3

2.4.1.1.2.2 CHART Archive Database Entity Relationship Diagram (ERD)

CHART ATMS Archive Database entity relationship diagrams are shown below in the multiple pages of figures labeled collectively as one Figure. These diagrams represent the archive database design for CHART ATMS R13.

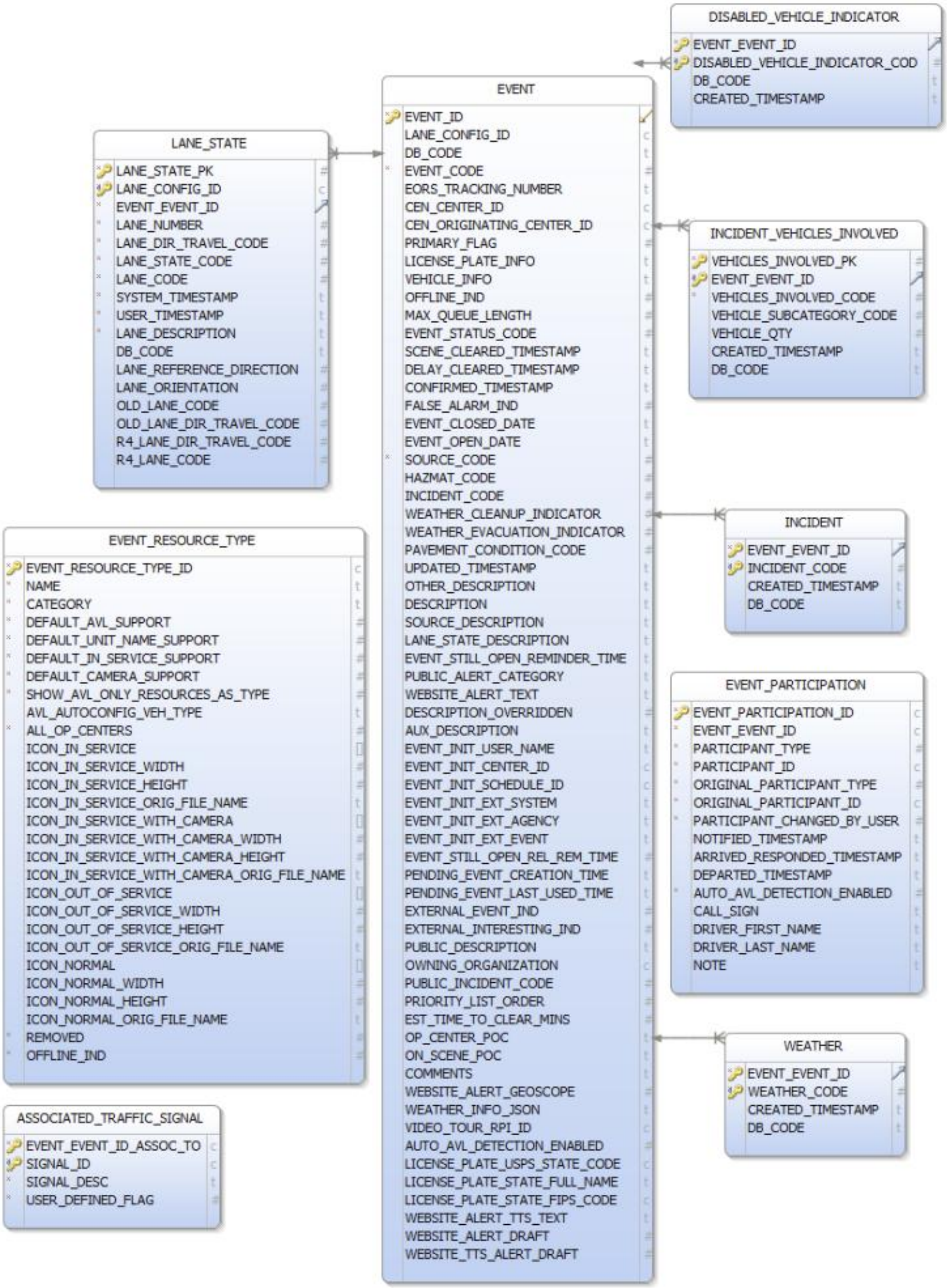


Figure 2-18. CHART_Archive ERD, Page 1-1

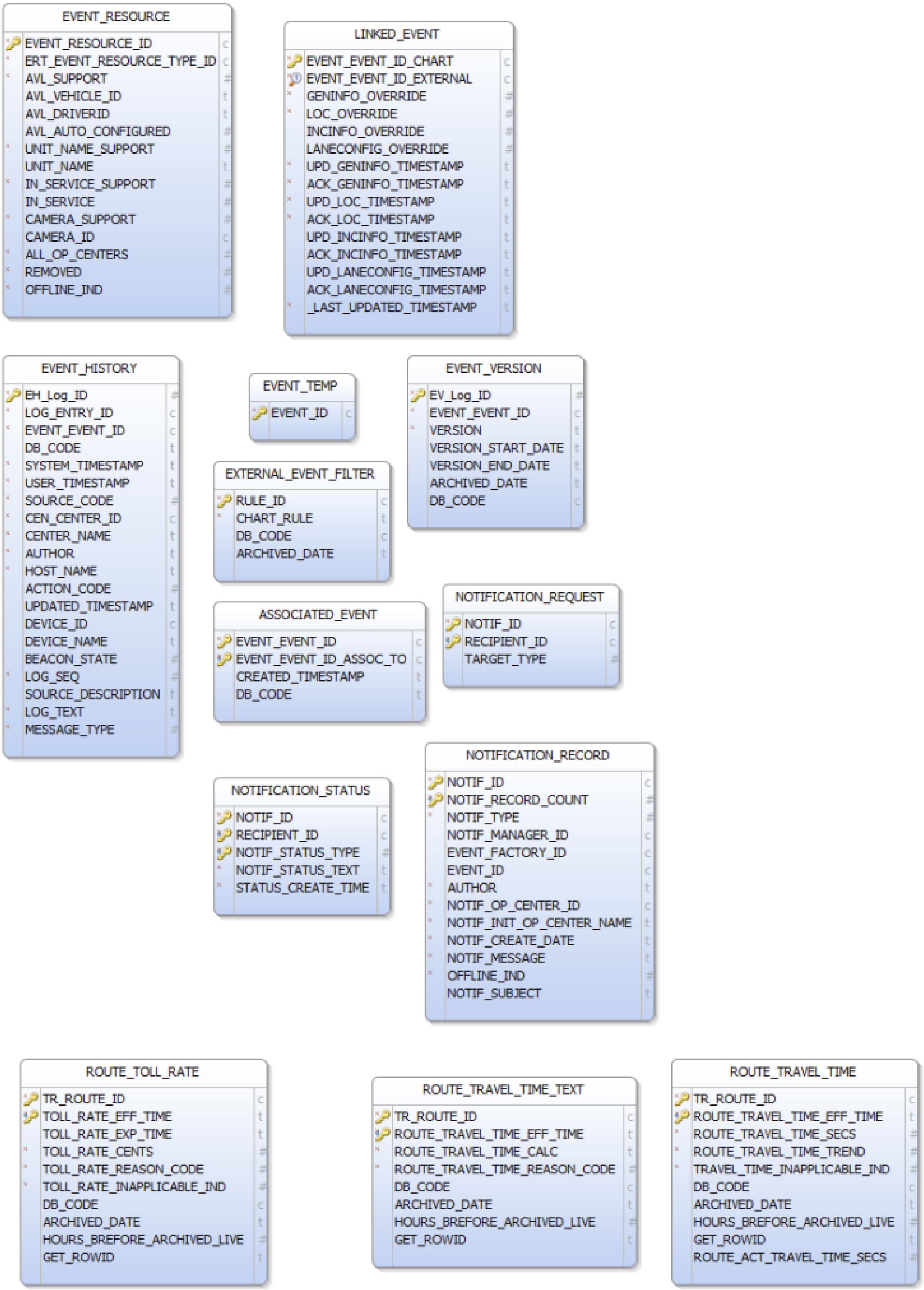


Figure 2-19. CHART_Archive ERD, Page 1-2

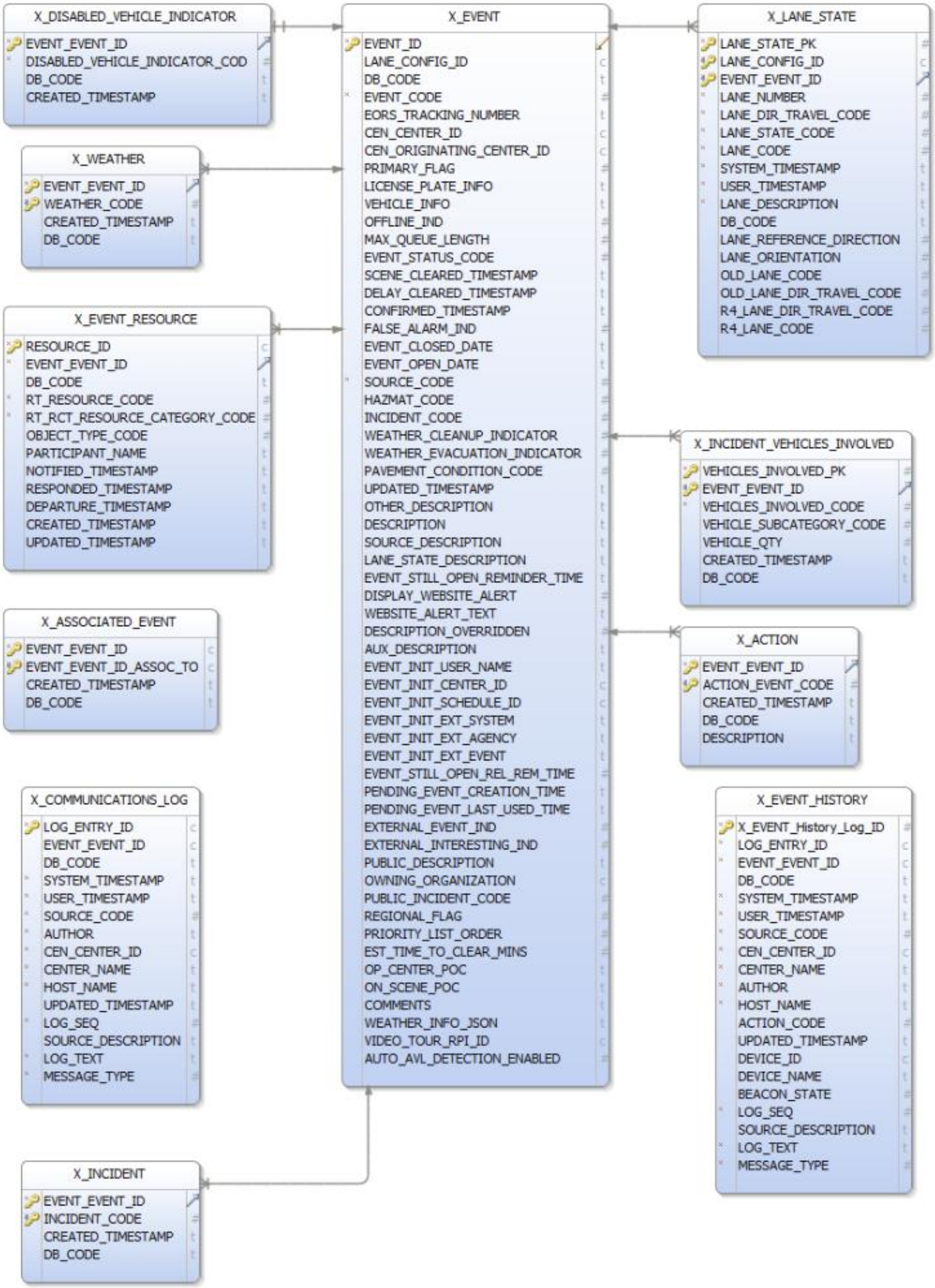


Figure 2-20. CHART_Archive ERD, Page 1-3

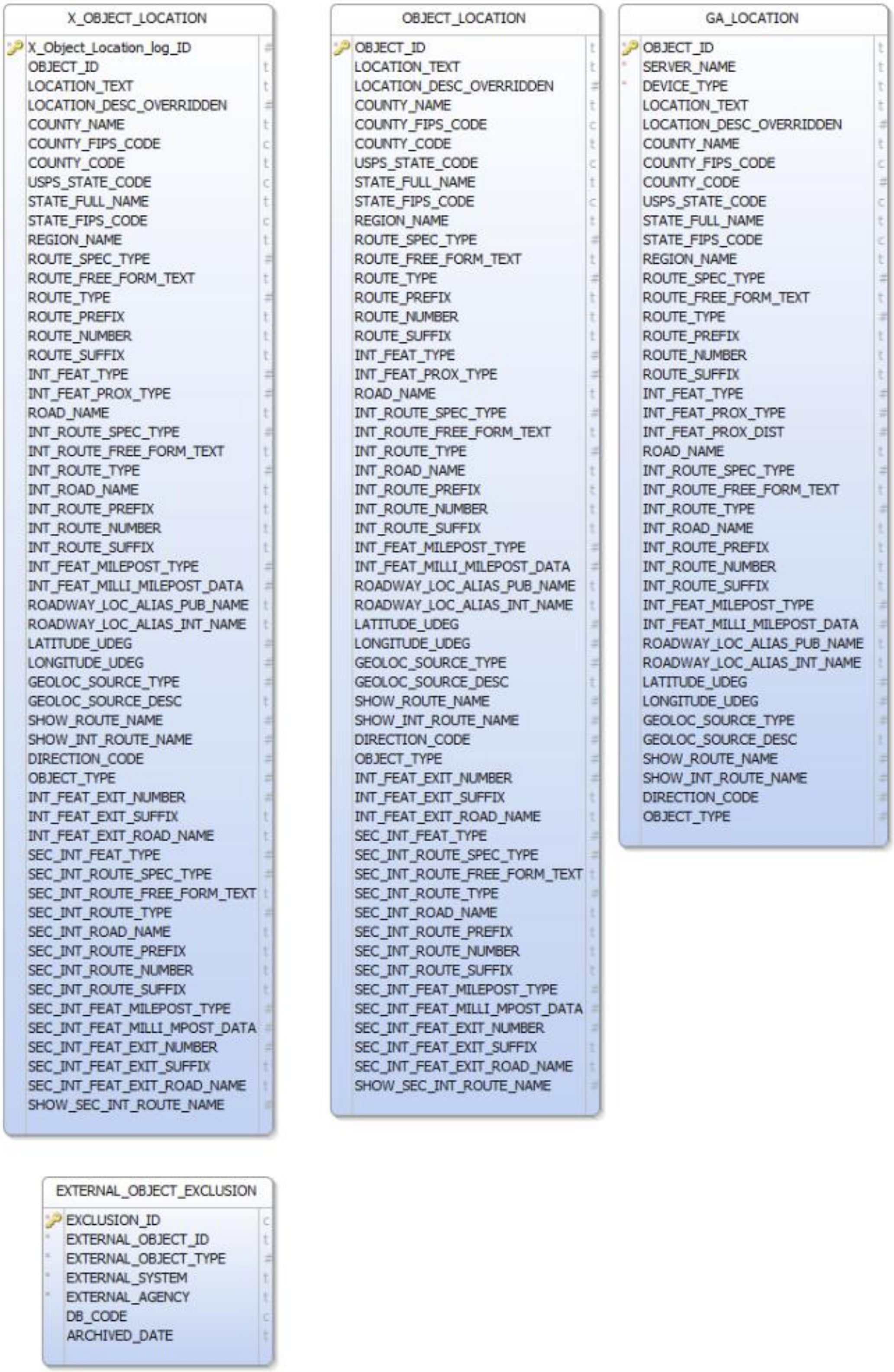


Figure 2-21. CHART_Archive ERD, Page 1-4

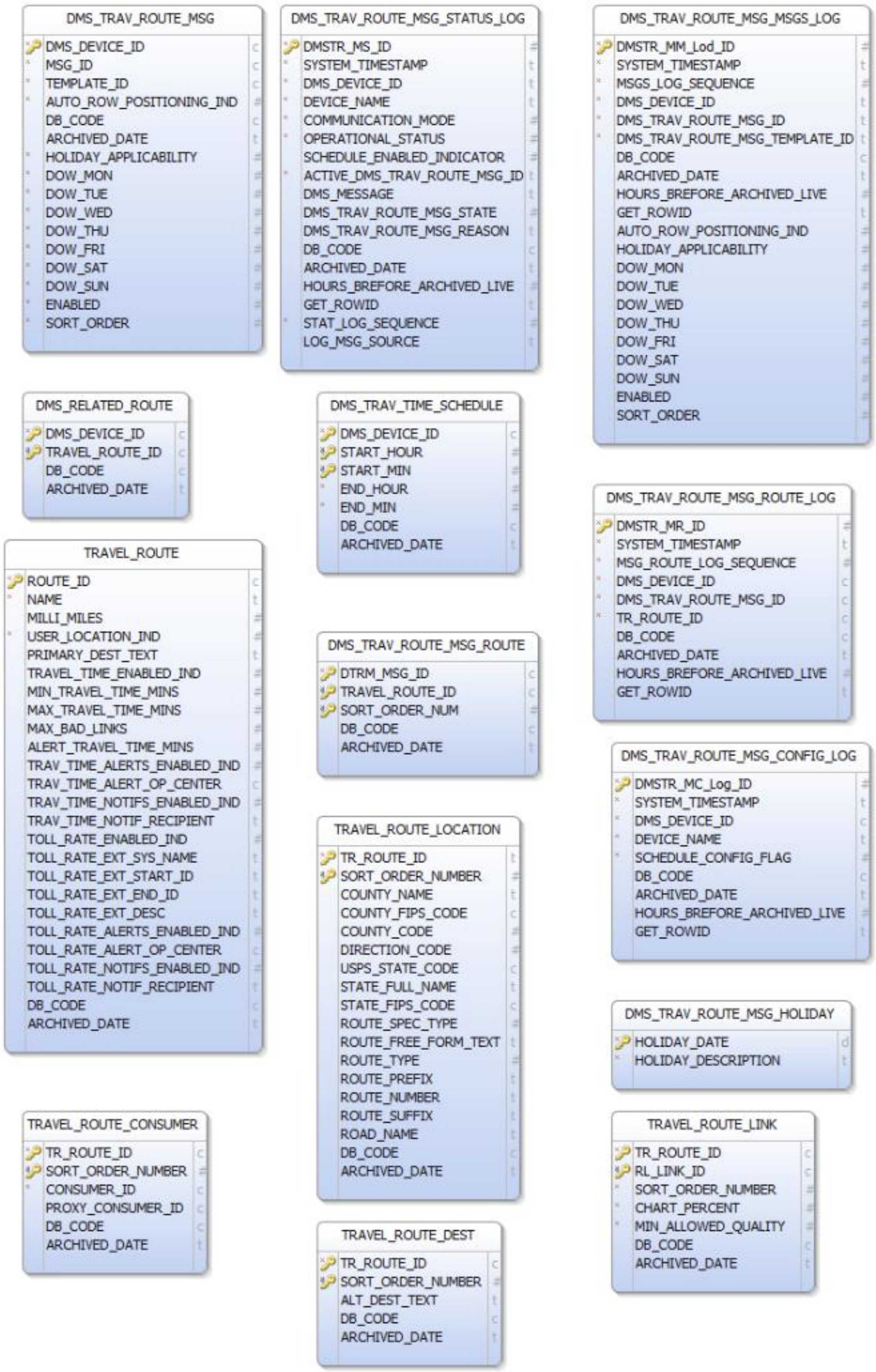


Figure 2-22. CHART_Archive ERD, Page 2-1

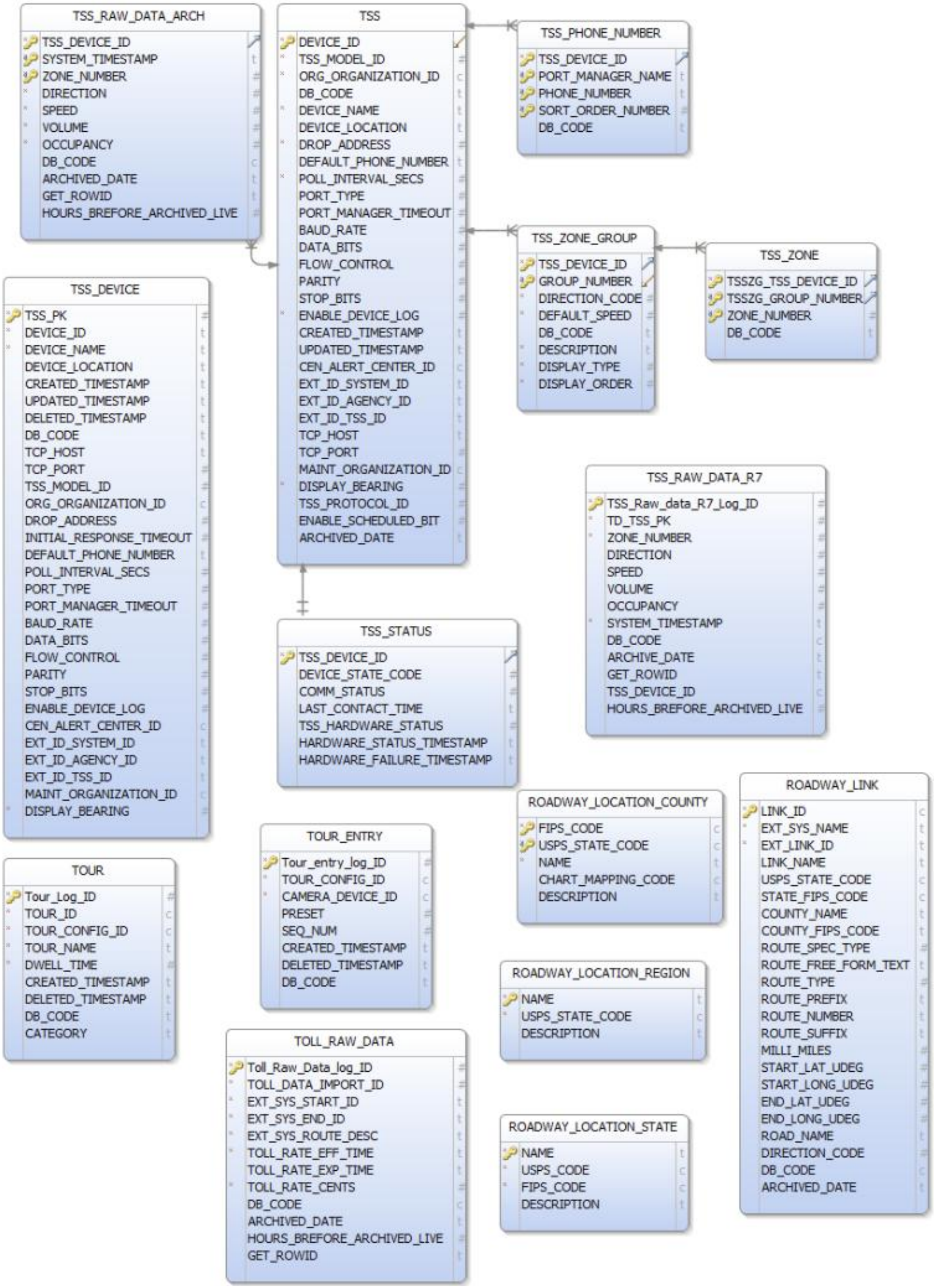


Figure 2-23. CHART_Archive ERD, Page 2-2

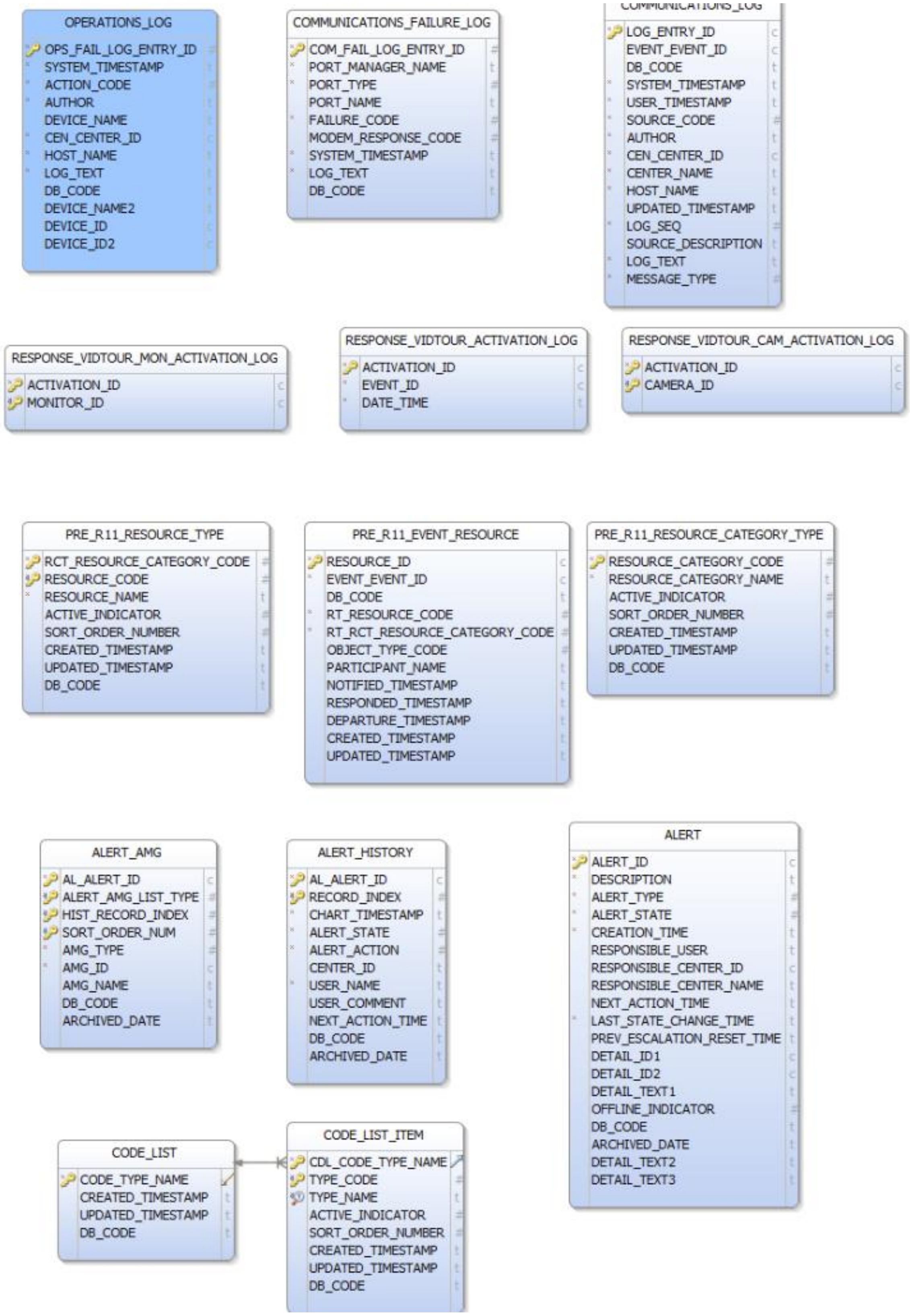


Figure 2-24. CHART_Archive ERD, Page 2-3

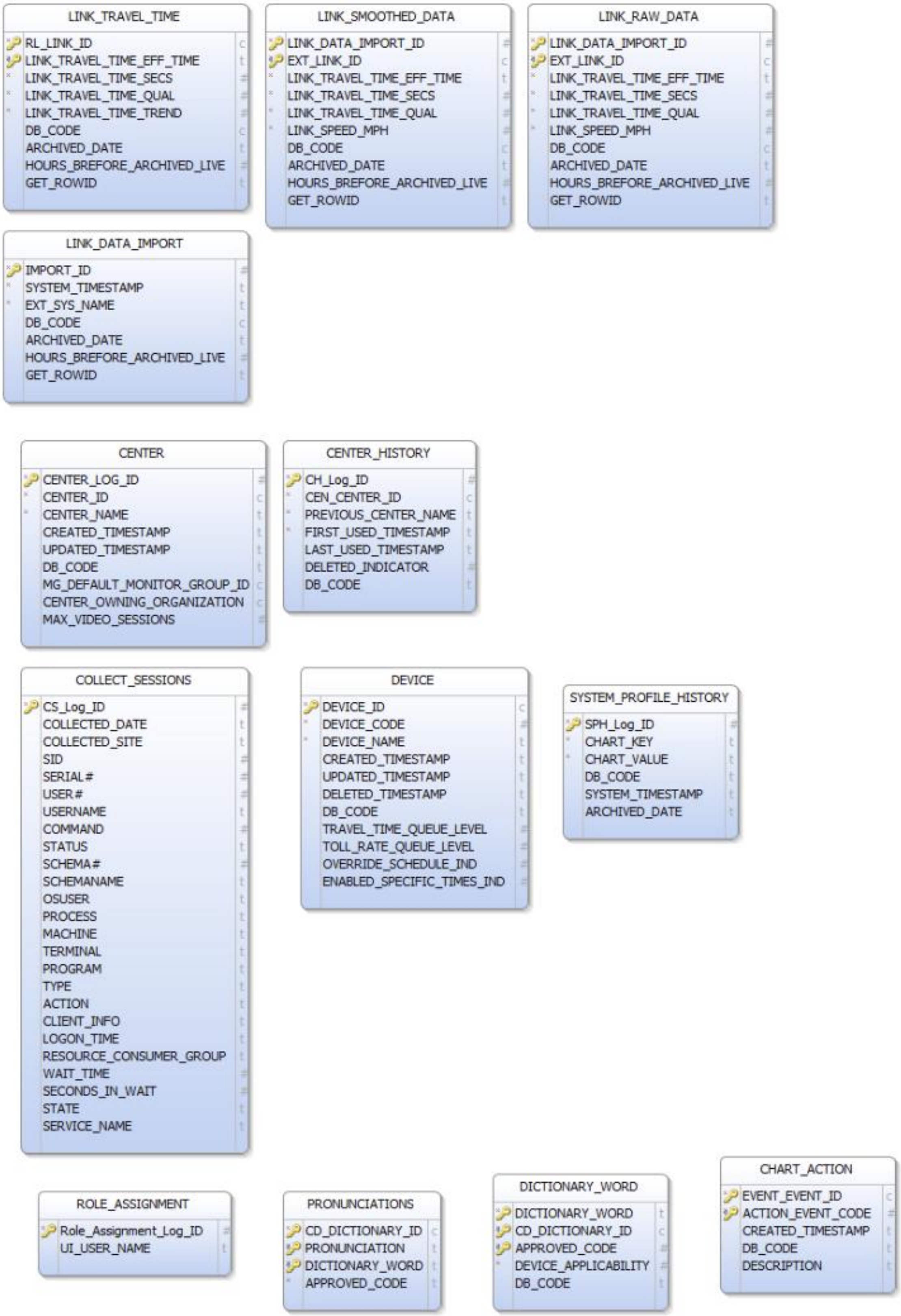


Figure 2-25. CHART_Archive ERD, Page 2-4

2.4.1.1.2.3 Function to Entity Matrix Report

The Create, Retrieve, Update, Delete (CRUD) matrix cross-references business functions to entities and shows the use of the entities by those functions. This report will be generated as part of the CHART O&M Guide.

2.4.1.1.2.4 Table Definition Report –

In tables shown below:

- Deleted columns/constraints marked with a minus sign ("-")
- Modified columns/constraints marked with an asterisk ("*")
- New columns/constraints marked with a plus sign ("+")

2.4.1.1.2.4.1 Database Changes for the Security Policy Enhancements Feature

2.4.1.1.2.4.1.1 CHART ATMS DB

The R13 Security Policy Enhancements feature requires changes to the USER_ID table and two new tables: a USER_PASSWORD table and a USER_FAILED_LOGIN table.

USER_FAILED_LOGIN Table (New):
Rights: The USERMANAGERSERVICE user requires full C/R/U/D rights for this table.

This new table stores information about failed attempts to login into user accounts. The failed attempts are accumulated because a sufficient number of failed logins within a brief period of time necessitates the account to be locked out for a few minutes prior to accepting another login attempt. (This slows down hacking attempts.) Note although UI_USER_NAME will normally reference back to a "parent" record in USER_ID, this may not always be the case. Failed logins are also stored for non-existent users. (This is so that hackers cannot glean any information about which accounts are valid accounts and which are non-existent by attempting a few logins on each candidate user account.) Therefore, UI_USER_NAME is not defined as a foreign key referencing USER_ID.

USER_FAILED_LOGIN Columns:

+UI_USER_NAME	VARCHAR(32)	NOT NULL
+CREATED_TIMESTAMP	DATETIME(2)	NOT NULL

USER_ID (Modified):
Rights: No changes for R12

This table is modified to store a flag to indicate which users are defined as "administrators" for the purpose of setting password policy for users (administrators have more stringent requirements for password length and for password expiration times); to store an account disabled indication (accounts can now be disabled and re-enabled); to store the time of last known logout; and to store the time (in the near future) when an account will be unlocked. (Note: a locked account is different from disabled account – a locked account is unlocked automatically at a predetermined time.) Also, the PASSWORD column is dropped from the USER_ID table (password information is now stored in a separate USER_PASSWORD table).

USER_ID Columns:

USER_NAME	VARCHAR(32)	NOT NULL
– PASSWORD	VARCHAR(32)	NOT NULL
DB_CODE	VARCHAR(1)	NULL
DEFAULT_CEN_CENTER_ID	CHAR(32)	NOT NULL
OTHER_CENTER_CAPABILITY	INT	NOT NULL
LAST_LOGIN_TIMESTAMP	DATETIME2(7)	NULL
LAST_LOGIN_CEN_CENTER_ID	CHAR(32)	NULL
+ LAST_LOGOUT_TIMESTAMP	DATETIME2(3)	NULL
+ ADMIN_INDICATOR	NUMERIC(1,0)	NOT NULL
+ DISABLED_INDICATOR	NUMERIC(1,0)	NOT NULL
+ UNLOCK_TIMESTAMP	DATETIME2(3)	NULL

PRIMARY KEY: USER_NAME

USER_PASSWORD Table (New):
Rights: The USERMANAGERSERVICE user requires full C/R/U/D rights for this table.

This new table stores the current password and recent previous passwords for each user, together with a timestamp indicating when the password was created.

USER_PASSWORD Columns:

+ UI_USER_NAME	VARCHAR(512)	NOT NULL
+ CREATED_TIMESTAMP	DATETIME2(3)	NOT NULL
+ PASSWORD	VARCHAR(32)	NOT NULL
+ ADMINISTRATIVELY_SET_INDICATOR	NUMERIC(1,0)	NOT NULL

PRIMARY KEY: UI_USER_NAME, CREATED_TIMESTAMP
FOREIGN KEY: UI_USER_NAME REFERENCES USER_ID.USER_NAME

2.4.1.1.2.4.2 Database Changes for the FITM Plans Feature

2.4.1.1.2.4.2.1 CHART ATMS DB

The R13 FITM Plans feature requires only one new functional right value.

FUNCTIONAL_RIGHT Table New Values:

FR_ID	FR_NAME	FR_DESCRIPTION
152	ViewFITMPlans	Allows the holder to view Freeway Incident Traffic Management (FITM) plans.

The only other database impact of the FITM Plans feature is that a traffic event history entry will be logged each time a user views a FITM plan (details / PDF file) from within the context of a traffic event.

2.4.1.1.2.4.3 Database Changes for the COTS Upgrades Feature

2.4.1.1.2.4.3.1 CHART ATMS DB

The R13 COTS Upgrades feature requires no changes to the CHART ATMS DB.

2.4.1.1.2.4.4 Database Changes for PR Fixes to be Included in R13

(PR fixes to be included in R13 have not yet been determined.)

2.4.1.1.2.5 Database Conversion

Prior to deploying R13, a script will need to be run to move passwords currently stored in USER_ID to the new USER_PASSWORD table. (Note: all passwords are and will continue to be stored only in encrypted form.)

2.4.1.1.2.6 PL/SQL Module Definition and Database Trigger Reports

There are no new PL/SQL modules for CHART ATMS R13.

2.4.1.1.2.7 Database Size Estimate - provides size estimate of current design

CHART ATMS R13 will cause a negligible increase in the size of the CHART ATMS database as follows:

- An anticipated 10 passwords will be stored per user instead of one password per user. That will add an estimated 16 K bytes to the database.
- Failed login attempts are stored only transiently, and will be cleared after the user logs in correctly or on a timer. An estimated 10 failed logins will occur per day, but the records are expected to remain in the system for only a minute, so there is no change in permanent database storage for this (excepting a brute force denial of service attack, which is not the normal case – but even in that case rows can be removed quickly on a timer).

2.4.1.1.2.8 Data Distribution

There are no changes to data distribution for R13.

2.4.1.1.2.9 Database Replication

Database replication is not used in R13.

2.4.1.1.2.10 Database Failover Strategy

The database failover strategy is defined as part of Work Order 27. There are no changes to the database failover strategy for R13.

2.4.1.1.2.11 Reports

No reports will be added or updated for R13. Since R5, the CHART reporting function has been transferred to University of Maryland.

2.4.1.2 CHART Flat Files

The following describes the use of flat files in CHART ATMS.

2.4.1.2.1 Service Registration Files

There are no service registration file changes for R13.

2.4.1.2.2 Service Property Files

Several new properties are expected to be stored in the UserManagementService.props file relating to password management. Properties expected to be stored in the UserManagementService.props file include:

UserManagementModule.AccountDisableDays (0 or 7-365, Default 60)
UserManagementModule.AccountDisableCheckFreqHours (0-168, Default 24)
UserManagementModule.BannedPasswordSequenceN (where N is 1,2,3,...) (no defaults)

2.4.1.2.3 GUI Property Files

There are only minor updates to the GUI properties file in its WEB-INF directory for CHART ATMS R13.

2.4.1.2.4 Device Logs

There are no changes to Device Log Files for CHART ATMS R13.

2.4.1.2.5 Service Process Logs

All CHART ATMS services write to a process log, used to provide a historical record of activity undertaken by the services. These logs are occasionally referenced by software engineering personnel to diagnose a problem or reconstruct a sequence of events leading to a particular anomalous situation. These logs are automatically deleted by the system after a set period of time defined by the service's properties file, so they do not accumulate infinitely. These files are stored in the individual service directories and are named by the service name and date, plus a "`.txt`" extension. These logs are typically read only by software engineering personnel. Except where noted, there are no changes for service process logs for R13 features.

2.4.1.2.6 Service Error Logs

All CHART ATMS services write to an error log, used to provide detail on certain errors encountered by the services. Most messages, including most errors, are captured by the CHART ATMS software and written to the process logs, but certain messages (typically produced by the Java Virtual Machine itself, by COTS, or DLLs) cannot be captured by CHART ATMS Software and instead are captured in these "catch-all" logs. Errors stored in these logs are typically problems resulting from a bad installation; once the system is up and running, errors rarely appear in these error logs. Debugging information from the JacORB COTS, which is not usually indicative of errors, can routinely be found in these error logs, as well. These log files can be reviewed by software engineering personnel to diagnose an installation problem or other type of problem. These logs are automatically deleted by the system after a set period of time defined by the service's properties file, so they do not accumulate infinitely. These files are stored in the individual service directories and are named by the service name and date, plus an ".err" extension. These logs are typically read only by software engineering personnel. Except where noted, there are no changes for service error logs for R13 features.

2.4.1.2.7 GUI Process Logs

Like the CHART background services, the CHART ATMS GUI service also writes to a process log file, used to provide a historical record of activity undertaken by the process. These GUI process logs are occasionally referenced by software engineering personnel to diagnose a problem or reconstruct a sequence of events leading to a particular anomalous situation. These logs are automatically deleted by the system after a set period of time defined by the GUI service's properties file, so they do not accumulate infinitely. These files are stored in the `chartlite/LogFiles/` directory under the `WebApps/` directory in the Apache Tomcat installation area. They are named by the service name ("`chartlite`") and date, plus a "`.txt`" extension. These logs are typically read only by software engineering personnel. Additional log files written by the Apache Tomcat system itself are stored in the `log/` directory in the Apache Tomcat installation area.

- The CHART ATMS R13 GUI changes do not change the way the GUI process logs operate.

2.4.1.2.8 FMS Port Configuration Files

The CHART ATMS Communications Services read a Port Configuration file, typically named `PortConfig.xml`, upon startup, which indicates which ports are to be used by the service and how they are to be initialized. A Port Configuration Utility is provided which allows for addition, removal of ports and editing of initialization parameters. As indicated by the extension, these files are in XML format. This means these files are hand-editable, although the Port Configuration Utility allows for safer, more controlled editing. The Port Configuration files are typically modified only by software engineers or telecommunications engineers.

- There are no changes to this section for the any of the CHART ATMS R13 features.

2.4.1.2.9 Watchdog Configuration Files

The watchdog configuration files will be updated for R13 to watch the new FITM web service.

2.4.2 Database Design

Changes made to the CHART ATMS database design for Release 13 features are described below.

2.4.2.1 CHART ATMS DB

2.4.2.1.1 Security Policy Enhancements Feature

The R13 Security Policy Enhancements feature will require two new tables and modifications to one table. See the details described in section 2.4.1.1.2.4.1 above.

2.4.2.1.2 FITM Plans Feature

The R13 FITM Plans feature will require one new functional right. See the details described in section 2.4.1.1.2.4.1 above.

2.4.2.2 Archiving - Changes

The CHART ATMS Archive database stores data from the CHART operational system as part of a permanent archive. The CHART ATMS Archive database design is a copy of the CHART ATMS operational system for those tables containing system, alert, traveler information messages and their underlying data, and event log information. In addition, the CHART ATMS Archive database stores detector data. No changes to archiving are required for R13.

3 Key Design Concepts

3.1 Security Policy Enhancements

The Security Policy Enhancements design is quite straightforward and involves very little complexity. An important consideration is that all new security features are configurable. Features may need to be adjusted based on changes to policy, and the features which add any significant burden to CHART ATMS users and/or administrators can be disabled, in the event that policies are lifted, waived, or found to be not applicable. Curently configured password rules will be enumerated on the pages where passwords are defined, so that users can be reminded of the rules which apply. Error messages will indicate all problems found with proposed new passwords at the same time, so that users are not forced into a cycle of discovering and fixing one password problem at a time. The specific parts of the proposed new passwords will not be displayed, as that could be found to be in violation of a rule which prohibits display of passwords at any time, but each individual rule violated will be indicated in the error message. Most of the password validity checking will be done on the server side, as some checks involve a fair bit of processing power, external dictionary, etc. Tthis way all password checking can be done in one place, and all violations of password rules can be indicated at once, rather than making users to find out in two phases what is wrong with proposed new passwords. Multiple password requirements involve classifying characters as letters, digits, or special characters, so this will be done only once per password, and the breakdown will be analyzed multiple times for the various rules.

3.2 FITMs

The FITM design is quite straightforward and involves very little complexity. The requirements decision to search for nearby FITM plans using a radius (i.e., straight-line distance as opposed to attempting to traverse the road network) greatly simplified the problem. Using straight-line distance, the ATMS GUI only makes a single query per discovery cycle to the new FITM mapping web service to get the metadata for all FITM plans in the system. The information is cached in ATMS GUI memory, and the coordinates associated with each FITM are used to find the FITM plans close to a traffic event.

3.3 COTS Upgrades

There is no design necessary for the COTS Upgrades.

3.4 Packaging

3.4.1 CHART ATMS

This software design is broken into packages of related classes. Table 3-1shows each package that is new or changed to support the Release 13 features.

Table 3-1. CHART ATMS Packages

Package Name	Package Description

Package Name	Package Description
CHART2.ResourceManagement	This IDL package is changed to support new password requirements and security features.
CHART2.ResourceModule	This package is changed to support new password requirements and security features.
CHART2.UserManagemet	This IDL package is changed to support new password requirements and security features.
CHART2.UserManagementModule	This package is changed to support new password requirements and security features.
CHART2.Utility	This package is changed to support new password requirements and security features.
chartlite.data.fitm	This package is new to support the caching of FITM data.
chartlite.servlet.fitm	This package is new to support FITM-related requests.
Chartlite.servlet.usermgnt	This package is changed to support new password requirements and security features.

3.5 Assumptions and Constraints

3.5.1 Security Policy Enhancements

There are no assumptions or constraints for Security Policy Enhancements.

3.5.2 FITM Plans

There are no assumptions or constraints for FITM Plans.

3.5.3 COTS Upgrades

There are no assumptions or constraints for COTS Upgrades.

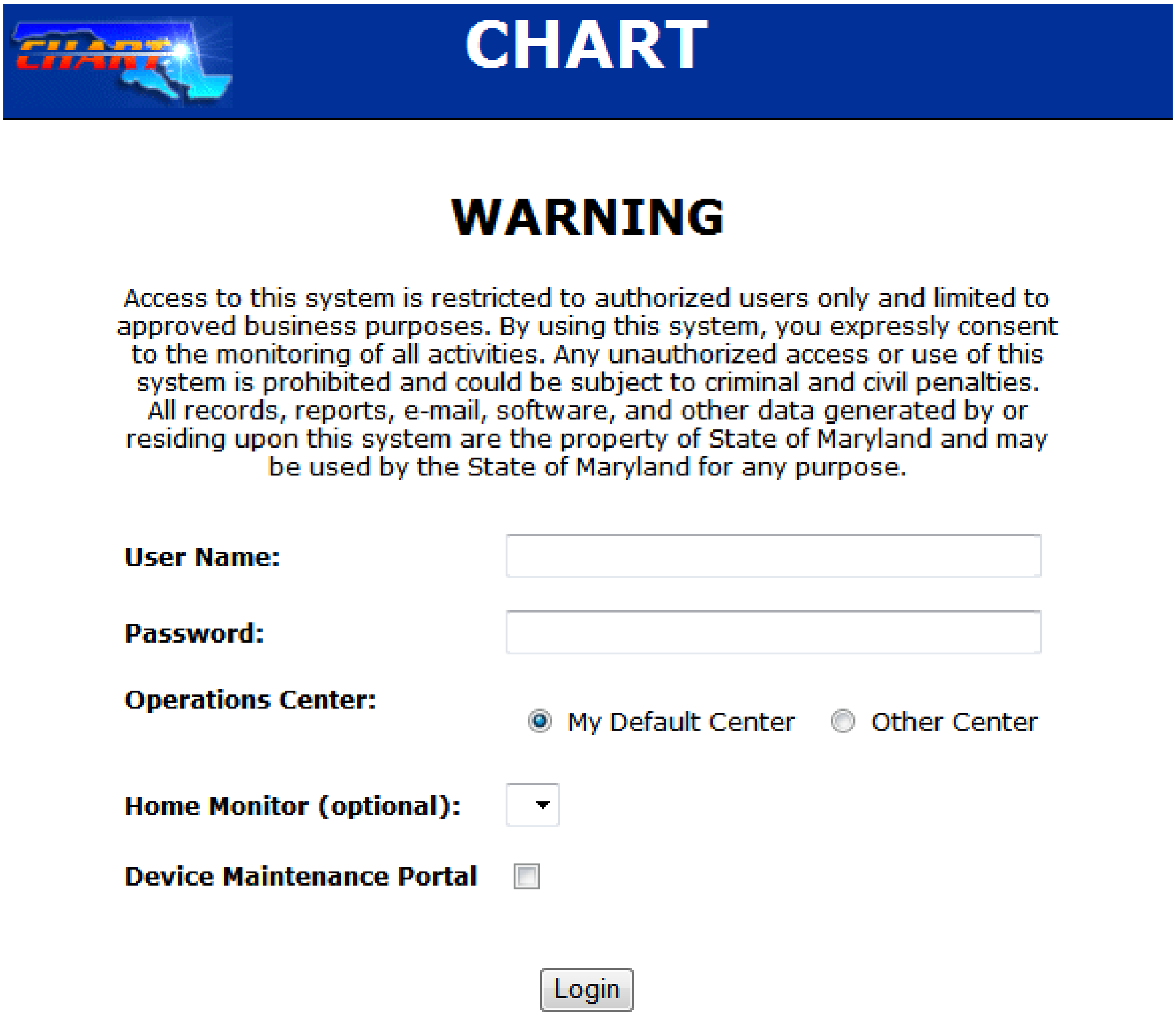
4 Human Machine Interface

4.1 Security Policy Enhancements Feature

This section describes the user interface changes in R13 related to the Security Policy Enhancements feature.

4.1.1 Display Warning on Login Screen

The CHART ATMS displays a usage warning on the login screen. An example is shown in Figure 4-1.



WARNING

Access to this system is restricted to authorized users only and limited to approved business purposes. By using this system, you expressly consent to the monitoring of all activities. Any unauthorized access or use of this system is prohibited and could be subject to criminal and civil penalties. All records, reports, e-mail, software, and other data generated by or residing upon this system are the property of State of Maryland and may be used by the State of Maryland for any purpose.

User Name:

Password:

Operations Center: ● My Default Center ○ Other Center

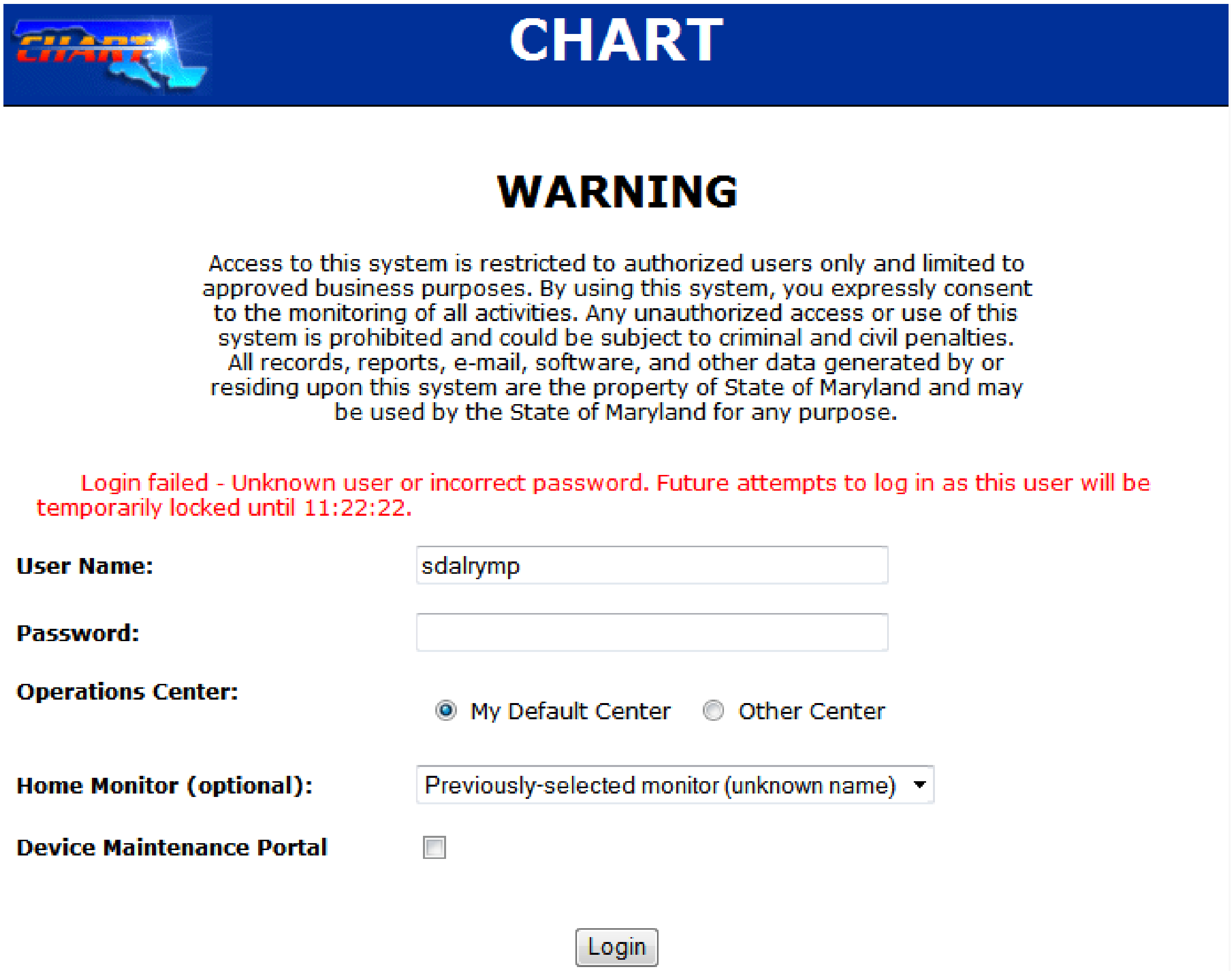
Home Monitor (optional):

Device Maintenance Portal □

Figure 4-1. Login Warning Caption

4.1.2 Delay Repeated Failed Login Attempts

The CHART ATMS will reduce the speed at which a hacker can attempt to break into the ATMS by introducing a delay, or a lockout, after a certain number of consecutive failed login attempts. 2013 Security Policy dictates that after 4 failed login attempts within a 15-minute period, the account must be locked for a period of 10 minutes. These values are configurable via System Profile. During this lock-out period, login attempts will not even be submitted from the web server to the User Manager Service. (If an attempt is made from another web server, the User Manager Service also knows about the lock-out and will still abort the attempt due to lockout.) An example of a message that will be provided is shown in Figure 4-2.



CHART

WARNING

Access to this system is restricted to authorized users only and limited to approved business purposes. By using this system, you expressly consent to the monitoring of all activities. Any unauthorized access or use of this system is prohibited and could be subject to criminal and civil penalties. All records, reports, e-mail, software, and other data generated by or residing upon this system are the property of State of Maryland and may be used by the State of Maryland for any purpose.

Login failed - Unknown user or incorrect password. Future attempts to log in as this user will be temporarily locked until 11:22:22.

User Name:	sdalrymp
Password:	
Operations Center:	● My Default Center ○ Other Center
Home Monitor (optional):	Previously-selected monitor (unknown name) ▾
Device Maintenance Portal	□

Figure 4-2. Lock-out Due to Failed Login Attempts

4.1.3 Show Last Successful Login/Logout Times Upon Login

When a user logs into the ATMS, the GUI will display the time of the most recent successful login and the time of the most recent successful logout. An observant user may notice a login/logout that he or she did not initiate. (Note that the last successful logout could be earlier than the last successful login, as there are ways to exit the system without a successful logout.) This is shown in Figure 4-3.

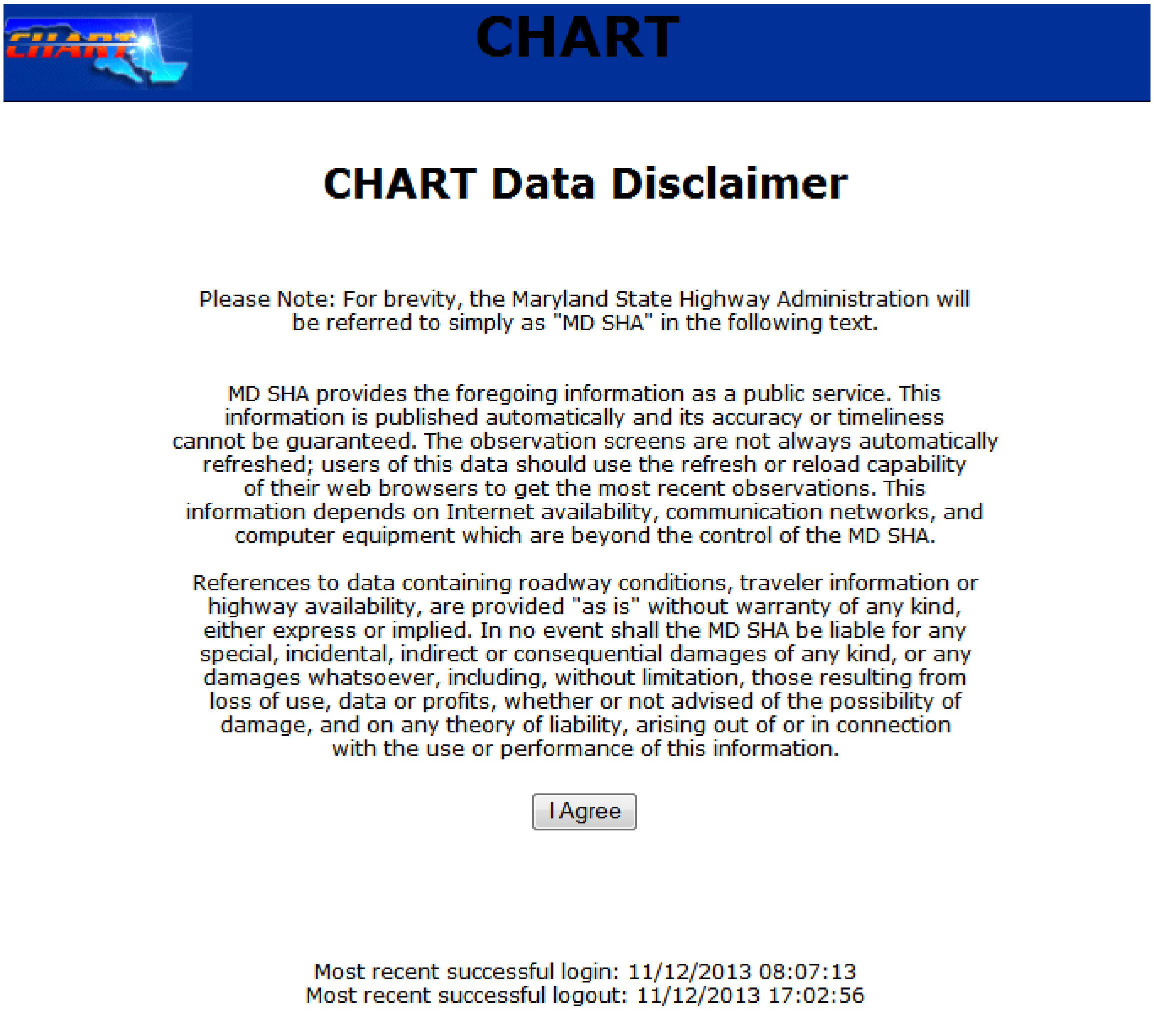


CHART Data Disclaimer

Please Note: For brevity, the Maryland State Highway Administration will be referred to simply as "MD SHA" in the following text.

MD SHA provides the foregoing information as a public service. This information is published automatically and its accuracy or timeliness cannot be guaranteed. The observation screens are not always automatically refreshed; users of this data should use the refresh or reload capability of their web browsers to get the most recent observations. This information depends on Internet availability, communication networks, and computer equipment which are beyond the control of the MD SHA.

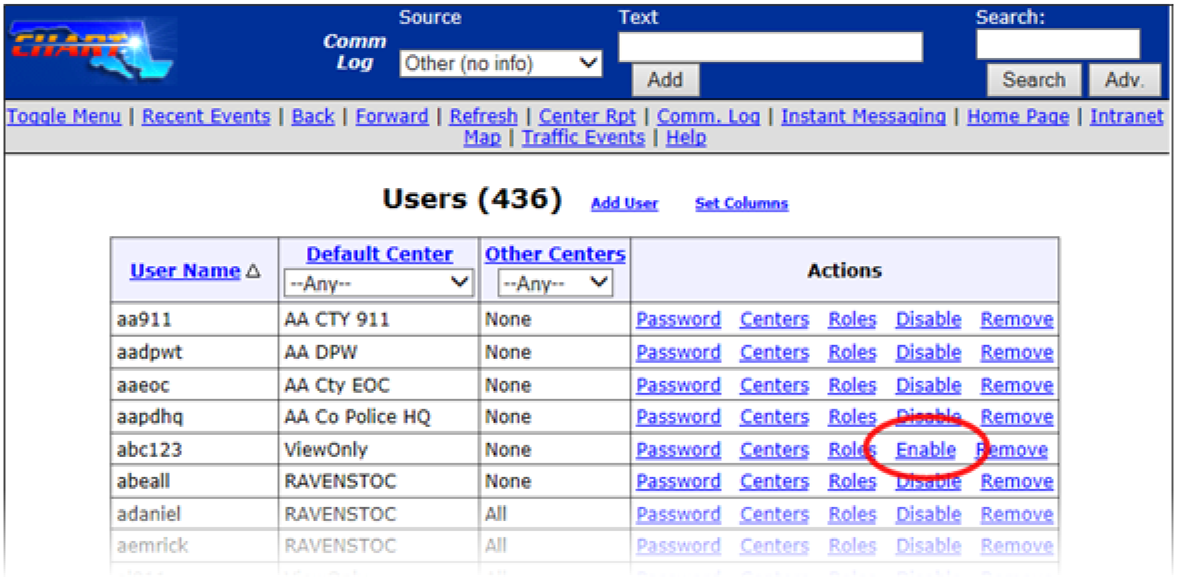
References to data containing roadway conditions, traveler information or highway availability, are provided "as is" without warranty of any kind, either express or implied. In no event shall the MD SHA be liable for any special, incidental, indirect or consequential damages of any kind, or any damages whatsoever, including, without limitation, those resulting from loss of use, data or profits, whether or not advised of the possibility of damage, and on any theory of liability, arising out of or in connection with the use or performance of this information.

Most recent successful login: 11/12/2013 08:07:13
Most recent successful logout: 11/12/2013 17:02:56

Figure 4-3. Last Successful Login/Logout Times

4.1.4 Disable Unused Accounts

The CHART ATMS disables accounts which have not been used for an extended period of time. 2013 Security Policy dictates that accounts be disabled after 60 days. Once an account has been disabled, a user with the Configure Users right must manually enable the account before it can be used again. Users with the Configure Users AND Manage User Logins rights can also manually disable accounts. This is shown in Figure 4-4. In the figure, the account for user “abc123” has been disabled. Consequently an “Enable” action (see red oval) is available for that user. All other users have a “Disable” action.


Source
Comm Log
Other (no info)
Text
Add
Search:
Search
Adv.
Toggle Menu | Recent Events | Back | Forward | Refresh | Center Rpt | Comm. Log | Instant Messaging | Home Page | Intranet
Map | Traffic Events | Help
Add User
Set Columns

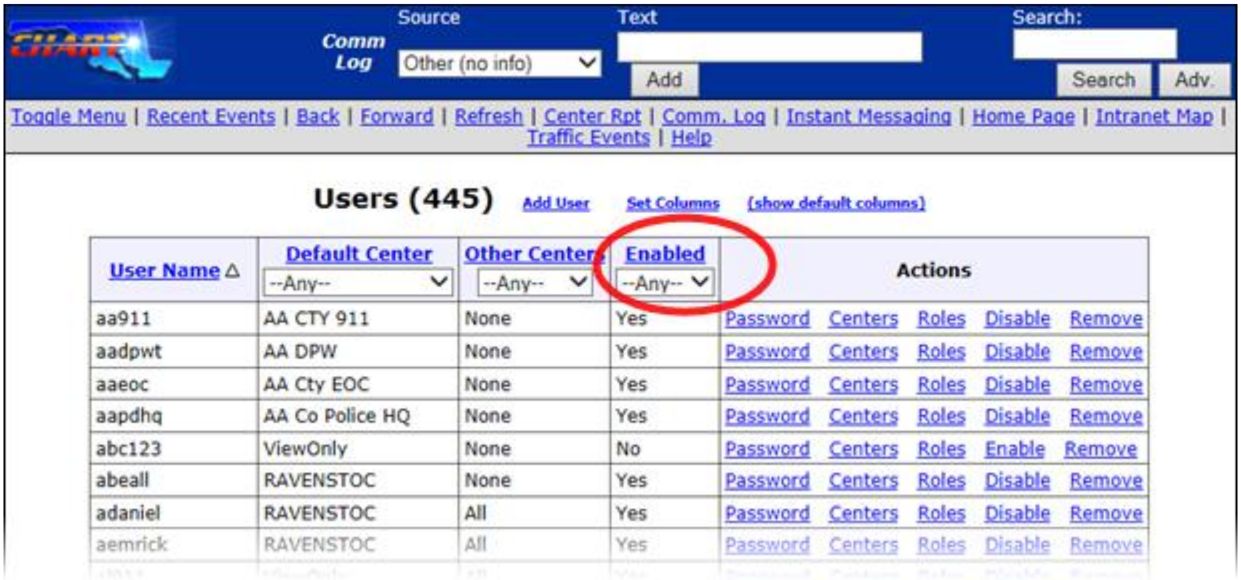
Users (436)

User Name △	Default Center --Any--	Other Centers --Any--	Actions
aa911	AA CTY 911	None	Password Centers Roles Disable Remove
aadpwt	AA DPW	None	Password Centers Roles Disable Remove
aaeoc	AA Cty EOC	None	Password Centers Roles Disable Remove
aapdhq	AA Co Police HQ	None	Password Centers Roles Disable Remove
abc123	ViewOnly	None	Password Centers Roles Enable Remove
abeall	RAVENSTOC	None	Password Centers Roles Disable Remove
adaniel	RAVENSTOC	All	Password Centers Roles Disable Remove
aemrick	RAVENSTOC	All	Password Centers Roles Disable Remove

Figure 4-4. Enable/Disable User capt

Note that to allow for space for the Enable/Disable links, we have shortened the names of links that existed prior to R13 as follows. "Set Password" has been changed to "Password". "View/Set Centers" has been changed to "Centers". "View/Set Roles" has been changed to "Roles".

An “Enabled” column is available for display. If “Set Columns” is clicked, the user can select “Enabled”, which adds a filterable “Enabled” column to the display. Users can then filter on “No” (or “Yes”) to see only user that are current disabled (or enabled). See Figure 4-5.

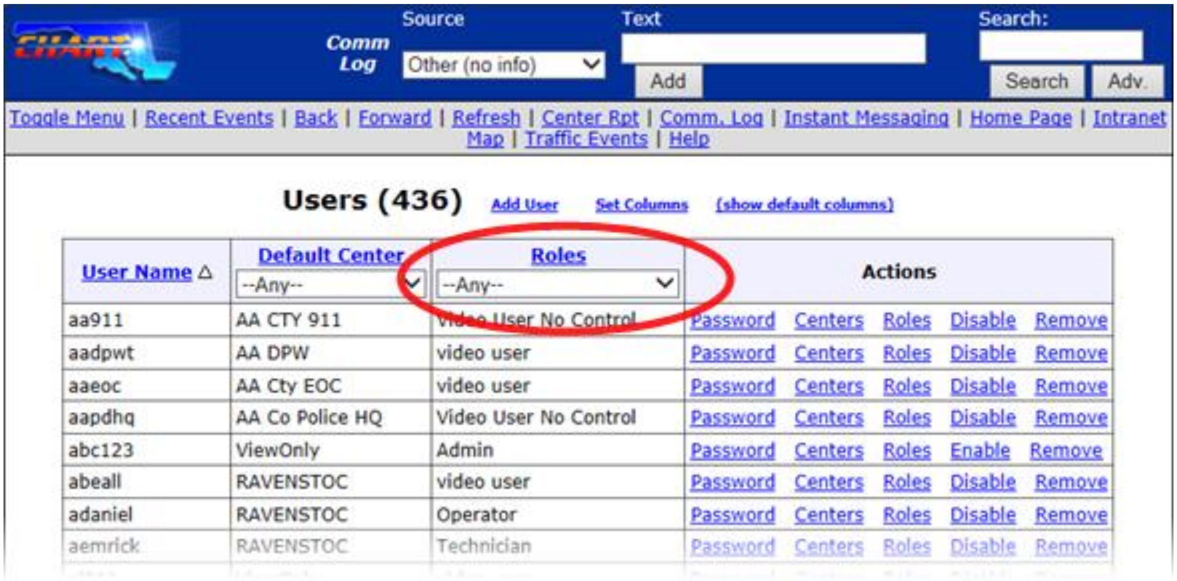

Source
Comm Log
Other (no info)
Text
Add
Search:
Search
Adv.
Toggle Menu | Recent Events | Back | Forward | Refresh | Center Rpt | Comm. Log | Instant Messaging | Home Page | Intranet Map | Traffic Events | Help
Add User
Set Columns
(show default columns)

Users (445)

User Name △	Default Center --Any--	Other Centers --Any--	Enabled --Any--	Actions
aa911	AA CTY 911	None	Yes	Password Centers Roles Disable Remove
aadpwt	AA DPW	None	Yes	Password Centers Roles Disable Remove
aaeoc	AA Cty EOC	None	Yes	Password Centers Roles Disable Remove
aapdhq	AA Co Police HQ	None	Yes	Password Centers Roles Disable Remove
abc123	ViewOnly	None	No	Password Centers Roles Enable Remove
abeall	RAVENSTOC	None	Yes	Password Centers Roles Disable Remove
adaniel	RAVENSTOC	All	Yes	Password Centers Roles Disable Remove
aemrick	RAVENSTOC	All	Yes	Password Centers Roles Disable Remove

Figure 4-5 Enabled Column in Users List capt

A “Roles” column is also available for display. If “Set Columns” is clicked, the user can select “Roles”, which adds a filterable “Roles” column to the display. Users can then filter on the roles assigned to user accounts. SeeFigure 4-6.

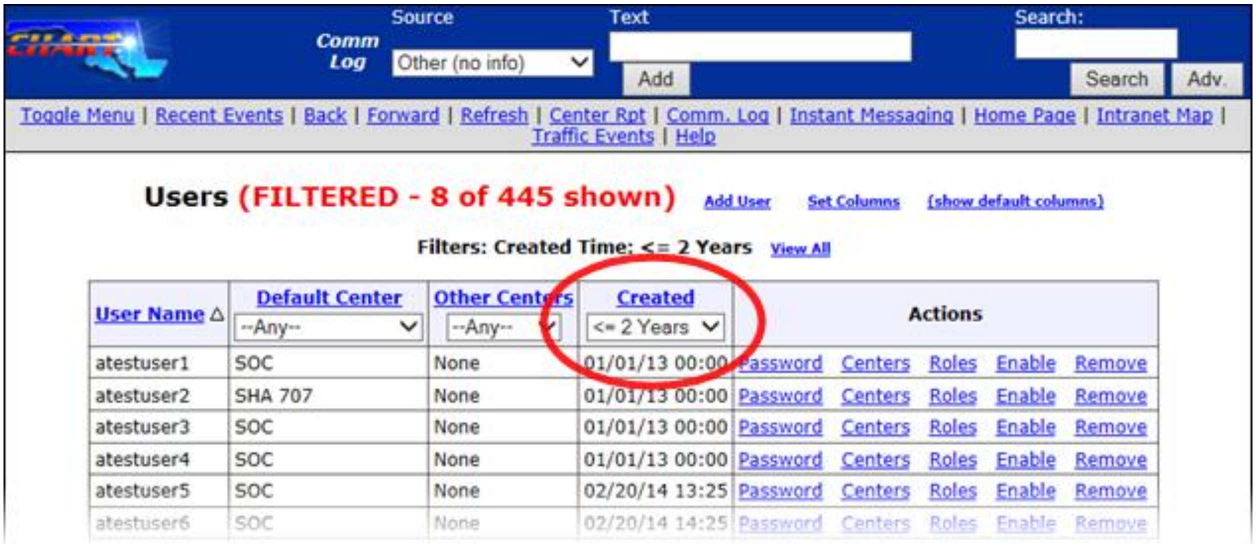

Source
Comm Log
Other (no info)
Text
Add
Search:
Search
Adv.
Toggle Menu | Recent Events | Back | Forward | Refresh | Center Rpt | Comm. Log | Instant Messaging | Home Page | Intranet Map | Traffic Events | Help
Add User
Set Columns
(show default columns)

Users (436)

User Name △	Default Center --Any--	Roles --Any--	Actions
aa911	AA CTY 911	Video User No Control	Password Centers Roles Disable Remove
aadpwt	AA DPW	video user	Password Centers Roles Disable Remove
aaeoc	AA Cty EOC	video user	Password Centers Roles Disable Remove
aapdhq	AA Co Police HQ	Video User No Control	Password Centers Roles Disable Remove
abc123	ViewOnly	Admin	Password Centers Roles Enable Remove
abeall	RAVENSTOC	video user	Password Centers Roles Disable Remove
adaniel	RAVENSTOC	Operator	Password Centers Roles Disable Remove
aemrick	RAVENSTOC	Technician	Password Centers Roles Disable Remove

Figure 4-6 Roles Column in Users List capt

A “Created” column is also available. If “Set Columns” is clicked, the user can select “Created”, which adds a filterable “Created” column to the display. Users can filter on a variety of time intervals to find user accounts that are newly created or those that have been in existence for a while. See Figure 4-7.


Comm Log
Source
Other (no info)
Text
Add
Search:
Search
Adv.
Toggle Menu | Recent Events | Back | Forward | Refresh | Center Rpt | Comm. Log | Instant Messaging | Home Page | Intranet Map | Traffic Events | Help
Add User
Set Columns
(show default columns)
View All

Users (FILTERED - 8 of 445 shown)

Filters: Created Time: <= 2 Years

User Name △	Default Center --Any--	Other Centers --Any--	Created <= 2 Years	Actions				
atestuser1	SOC	None	01/01/13 00:00	Password	Centers	Roles	Enable	Remove
atestuser2	SHA 707	None	01/01/13 00:00	Password	Centers	Roles	Enable	Remove
atestuser3	SOC	None	01/01/13 00:00	Password	Centers	Roles	Enable	Remove
atestuser4	SOC	None	01/01/13 00:00	Password	Centers	Roles	Enable	Remove
atestuser5	SOC	None	02/20/14 13:25	Password	Centers	Roles	Enable	Remove
atestuser6	SOC	None	02/20/14 14:25	Password	Centers	Roles	Enable	Remove

Figure 4-7 Created Column in Users List capt

4.1.5 Password Requirements

There are several password requirements for creation of new passwords. There are no screenshots for these, but the following requirements are enforced:

- **Password/User ID uniqueness:** The User ID cannot be contained in the password (for instance user “aworthington” and password “aworthingtonpw” is not valid) and the password cannot be contained within the user (user “aworthington” and password “Worthington” is not valid). This requirement cannot be disabled.

- **Password length:** The password must be a certain minimum length. The lengths are configurable. The length required for users designated as administrators can be different from the length required for normal users. 2013 Security Policy dictates a minimum length of 11 for administrators and 8 for normal users.

- **Password variety:** Passwords must have a certain variety of characters. The required number of characters of each type are configurable via system profile. Character types for which minimum numbers can be set are listed below. 2013 Security Policy is extremely weak in this regard, and may be expected to change.

    - **Letters (of any case).** 2013 Security Policy dictates at least one letter must be required.

    - **Upper case letters.** 2013 Security Policy does not specify a minimum number of uppercase letters.

  - **Lowercase letters.** 2013 Security Policy does not specify a minimum number of lowercase letters.

  - **Digits.** 2013 Security Policy dictates at least one digit must be required.

  - **Special characters.** 2013 Security Policy does not specify a minimum number of special characters. Also notable: spaces at the beginning and end of a password, which used to be ignored, are now strictly prohibited, and spaces within a password, which used to be illegal, are now legal.

- **Password changing:** When changing one's own password, the new password cannot be created only by adding a single character to the password, by deleting a single character from the password, or by changing a single character in the password. Each of these three requirements can be disabled via System Profile.

- **Password reuse:** When changing one's own password, the new password cannot have been recently used by that user. The number of passwords saved and checked is configurable via System Profile. 2013 Security Policy dictates that the new password cannot be the same as any of the previous ten passwords used by that user.

- **Password cycling:** A user is prohibited from changing his or her own password too rapidly. This is designed to prevent subverting the password reuse requirement. Otherwise a user could maintain a "favorite password", quickly cycling through ten passwords each time his/her password expires, returning back to his or her favorite password. 2013 Security Policy dictates that a password can be changed a maximum of one time within any two-day period. The time period and the number of changes allowed in that time period are configurable via System Profile. If a user has legitimate need to change his or her password, for instance if password compromise is suspected, an administrator can still reset the password (after which the user is allowed (and forced) to make another password change on the next login.

- **Password expiration:** Passwords expire after a certain number of days. The expiration times for users designated as administrators can be different from the expiration time for normal users, and are configurable via System Profile. 2013 Security Policy requires a 30-day expiration for administrators and a 45-day expiration for normal users.

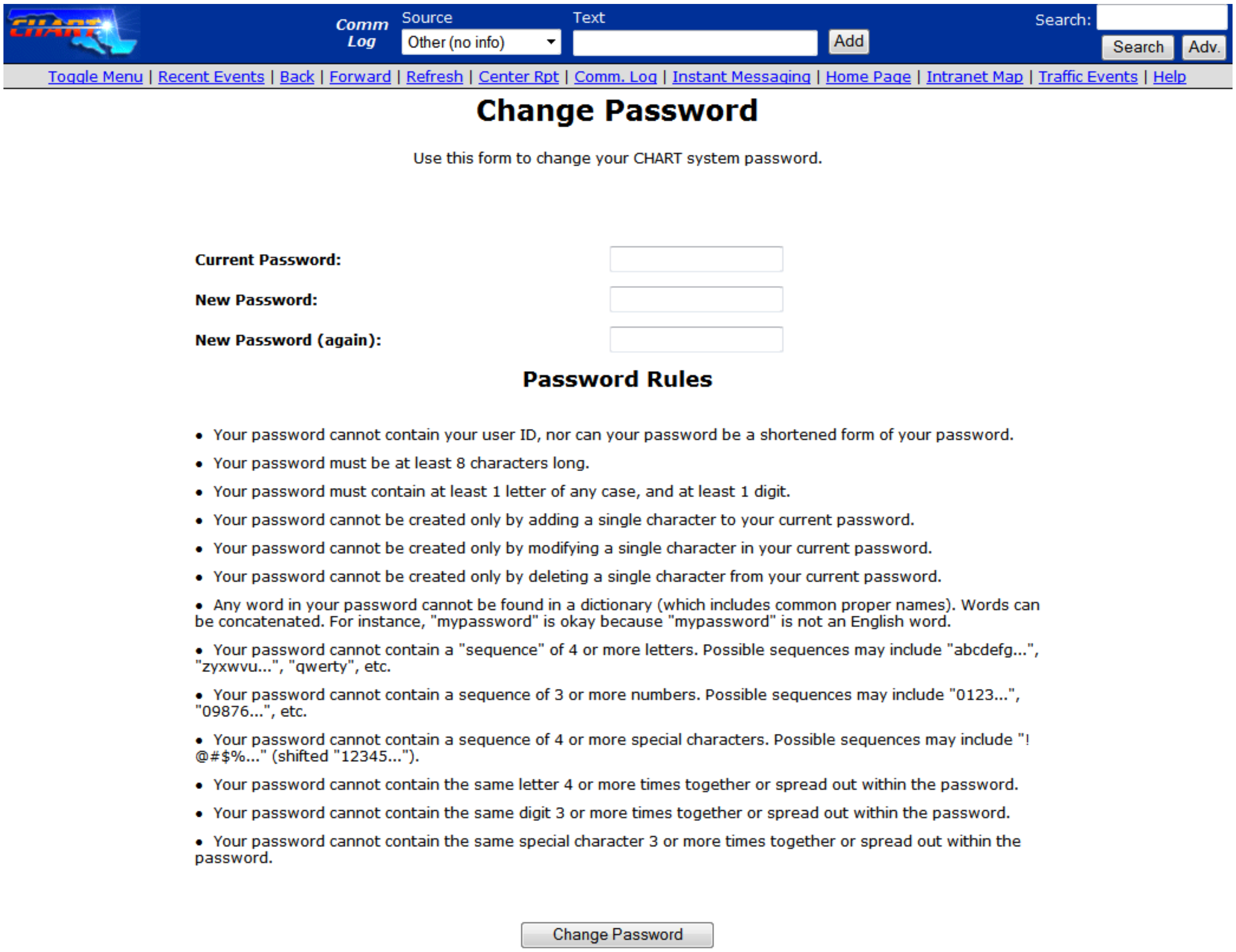
- **Password resets:** Whenever a user's password is set by an administrator (either upon account creation or due to a password reset), the user is forced to change his/her password the next time the user logs in. (The user can also elect to abort the login, and be logged out instead, but in order to gain access to the system, the user must immediately change the password.)

- **Password dictionary check:** Passwords cannot contain words found in a dictionary. The dictionary contains common English words and proper names. The strings which are searched are "maximal" strings of letters. For example, the password "my-password65" is invalid because both "my" and password" are found in the dictionary, but "mypassword65" is valid because "mypassword" is not found in the dictionary. The dictionary check can be disabled via System Profile.

- **Password sequences:** Passwords cannot contain "sequences" of letters, digits or numbers. The prohibited sequences are configurable via User Manager Service properties, and are expected to include alphabetic/numeric sequences, such as "abcdefg…" and "01234567890" (as well as these sequences in reverse, "zyxwvu…", etc.) and keyboard sequences, such as "qwertyuiop" and "!@#$%^&..." (shifted number sequence "1234567…"). The numbers of letters, numbers, and special characters considered invalid are also configurable via System Profile, and might be, for example 4 letters, 3 digits, and 4 special characters. (A limit of 3 for digits catches "number pad" sequences such as "789456123".) This rule is mandated in 2013 Security Policy, but the number of characters in sequence which is to be prohibited is not specified (it just says "no characters in sequence"). Policy says "no characters in sequence", implying two characters in sequence should be invalid, but this does not seem appropriate.

- **Password repeated characters:** Passwords cannot contain excessive repeated characters. For instances, passwords such as "a1a1a1a1", "fredfredfredfred1", and "MyPassss" should be considered invalid." The number of repeated letters, numbers, and special characters prohibited is configurable via system profile. This rule is mandated in 2013 Security Policy, but the number of repeated characters is not specified. Policy says "no repeated characters", implying two of the same character should be invalid, but this does not seem appropriate.

Password rules are indicated on the change password page, as shown in Figure 4-8. The rules displayed are dynamically updated as the password settings are configured in the System Profile. The applicable subset of rules is also shown on the administrator Set Password (for another user) and Add User pages (not shown here).


Comm Log
Source
Other (no info)
Text
Add
Search:
Search
Adv.
Toggle Menu | Recent Events | Back | Forward | Refresh | Center Rpt | Comm. Log | Instant Messaging | Home Page | Intranet Map | Traffic Events | Help

Change Password

Use this form to change your CHART system password.

Current Password:

New Password:

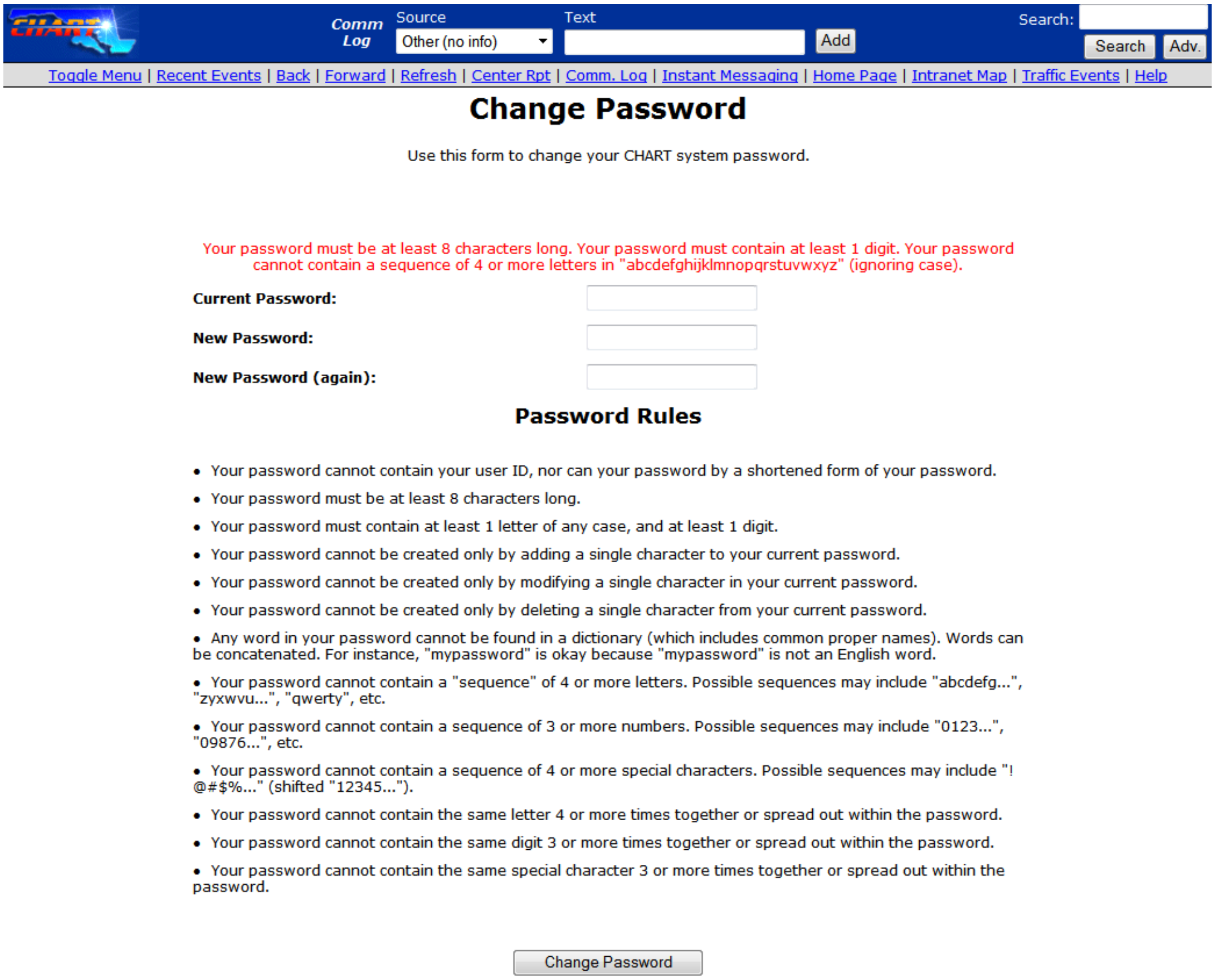
New Password (again):

Password Rules

- Your password cannot contain your user ID, nor can your password be a shortened form of your password.
- Your password must be at least 8 characters long.
- Your password must contain at least 1 letter of any case, and at least 1 digit.
- Your password cannot be created only by adding a single character to your current password.
- Your password cannot be created only by modifying a single character in your current password.
- Your password cannot be created only by deleting a single character from your current password.
- Any word in your password cannot be found in a dictionary (which includes common proper names). Words can be concatenated. For instance, "mypassword" is okay because "mypassword" is not an English word.
- Your password cannot contain a "sequence" of 4 or more letters. Possible sequences may include "abcdefg...", "zyxwvu...", "qwerty", etc.
- Your password cannot contain a sequence of 3 or more numbers. Possible sequences may include "0123...", "09876...", etc.
- Your password cannot contain a sequence of 4 or more special characters. Possible sequences may include "!@#$%..." (shifted "12345...").
- Your password cannot contain the same letter 4 or more times together or spread out within the password.
- Your password cannot contain the same digit 3 or more times together or spread out within the password.
- Your password cannot contain the same special character 3 or more times together or spread out within the password.

Figure 4-8. Change Password Dialog with Password Rules

If the password does not meet all the rules, the complete list of rules violated is provided to the user, as shown in Figure 4-9. No part of the user's proposed new password is shown, for security reasons.


Comm Log
Source
Other (no info)
Text
Add
Search:
Search
Adv.
Toggle Menu | Recent Events | Back | Forward | Refresh | Center Rpt | Comm. Log | Instant Messaging | Home Page | Intranet Map | Traffic Events | Help

Change Password

Use this form to change your CHART system password.

Your password must be at least 8 characters long. Your password must contain at least 1 digit. Your password cannot contain a sequence of 4 or more letters in "abcdefghijklmnopqrstuvwxyz" (ignoring case).

Current Password:

New Password:

New Password (again):

Password Rules

- Your password cannot contain your user ID, nor can your password by a shortened form of your password.
- Your password must be at least 8 characters long.
- Your password must contain at least 1 letter of any case, and at least 1 digit.
- Your password cannot be created only by adding a single character to your current password.
- Your password cannot be created only by modifying a single character in your current password.
- Your password cannot be created only by deleting a single character from your current password.
- Any word in your password cannot be found in a dictionary (which includes common proper names). Words can be concatenated. For instance, "mypassword" is okay because "mypassword" is not an English word.
- Your password cannot contain a "sequence" of 4 or more letters. Possible sequences may include "abcdefg...", "zyxwvu...", "qwerty", etc.
- Your password cannot contain a sequence of 3 or more numbers. Possible sequences may include "0123...", "09876...", etc.
- Your password cannot contain a sequence of 4 or more special characters. Possible sequences may include "!@#$%..." (shifted "12345...").
- Your password cannot contain the same letter 4 or more times together or spread out within the password.
- Your password cannot contain the same digit 3 or more times together or spread out within the password.
- Your password cannot contain the same special character 3 or more times together or spread out within the password.

Figure 4-9. Change Password Dialog with Password Violations

4.2 FITM Plans Feature

This section describes the user interface changes in R13 related to the Freeway Incident Traffic Management (FITM) Plans feature.

There are two new links for viewing the list of FITM plans:

- The FITM Plans link on the main menu shows the list of all FITM plans in the system.
- The View FITM Plans link on the Traffic Event Details page shows the FITM plans near the location of the traffic event (if the location of the event is defined), or all FITM plans in the system.

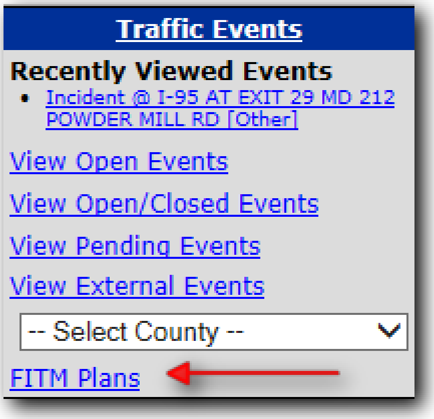
The links above are shown only if a user has the View FITM Plans functional right.

There is also a new System Profile screen for the new settings to specify the criteria for searching for FITM plans near a traffic event. This screen is available to users with the Configure System right.

The sections below provide details on all of the changes.

4.2.1 View All FITM Plans (Outside of Traffic Event)

A user with the View FITM Plans right can view the list of all FITM plans outside the context of an event. This functionality is invoked from the menu as shown in Figure 4-10.



Traffic Events

Recently Viewed Events

- Incident @ I-95 AT EXIT 29 MD 212 POWDER MILL RD [Other]

View Open Events

View Open/Closed Events

View Pending Events

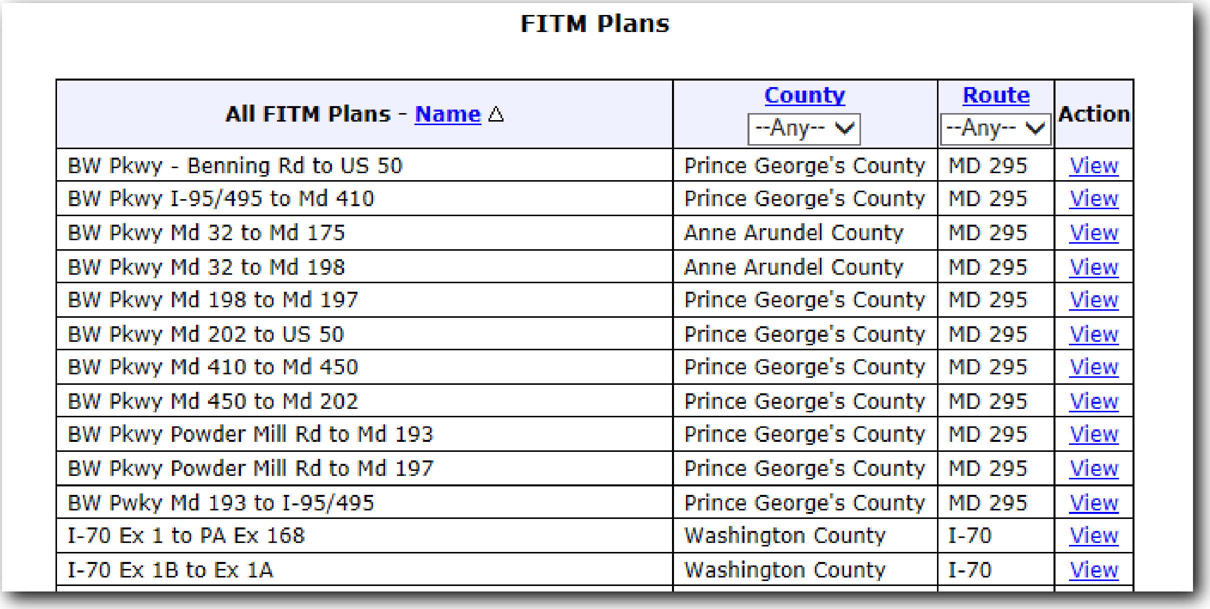
View External Events

-- Select County --

FITM Plans

Figure 4-10. FITM Plans Menu Item

The menu item brings up the screen showing all FITM plans as shown in Figure 4-11.



FITM Plans

All FITM Plans - Name △	County --Any--	Route --Any--	Action
BW Pkwy - Benning Rd to US 50	Prince George's County	MD 295	View
BW Pkwy I-95/495 to Md 410	Prince George's County	MD 295	View
BW Pkwy Md 32 to Md 175	Anne Arundel County	MD 295	View
BW Pkwy Md 32 to Md 198	Anne Arundel County	MD 295	View
BW Pkwy Md 198 to Md 197	Prince George's County	MD 295	View
BW Pkwy Md 202 to US 50	Prince George's County	MD 295	View
BW Pkwy Md 410 to Md 450	Prince George's County	MD 295	View
BW Pkwy Md 450 to Md 202	Prince George's County	MD 295	View
BW Pkwy Powder Mill Rd to Md 193	Prince George's County	MD 295	View
BW Pkwy Powder Mill Rd to Md 197	Prince George's County	MD 295	View
BW Pwky Md 193 to I-95/495	Prince George's County	MD 295	View
I-70 Ex 1 to PA Ex 168	Washington County	I-70	View
I-70 Ex 1B to Ex 1A	Washington County	I-70	View

Figure 4-11. All FITM Plans (Outside Event)

The list is initially sorted by Name. The user can sort the list by Name, County, or Route. The user can also filter the list by County or Route. Clicking on the View link invokes the detailed view of the FITM plan, which is described in the following section.

4.2.2 View FITM Plan (Details)

The user can click on the View link from a list of FITM plans to view the FITM plan details. The FITM plan itself is an Adobe PDF file containing a stylized map, turn-by-turn directions, and a list of affected traffic signals. A browser plugin capable of showing PDF files must be installed for this functionality to work. Figure 4-12 shows part of a FITM Plan PDF file.

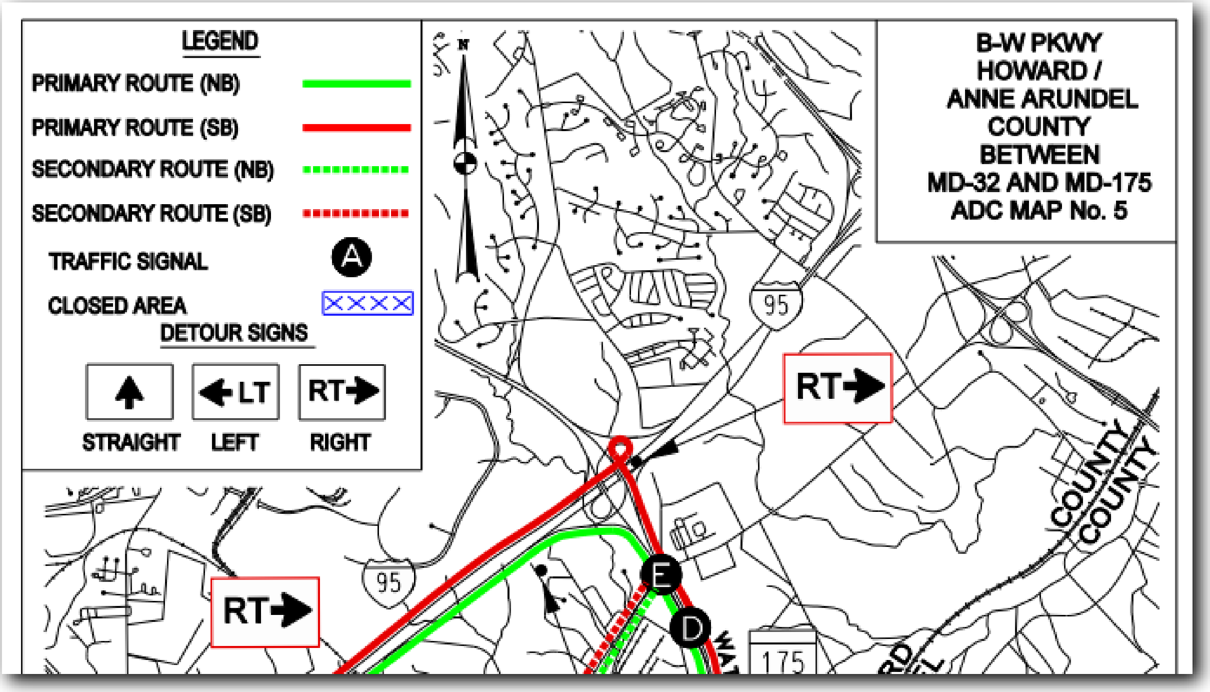
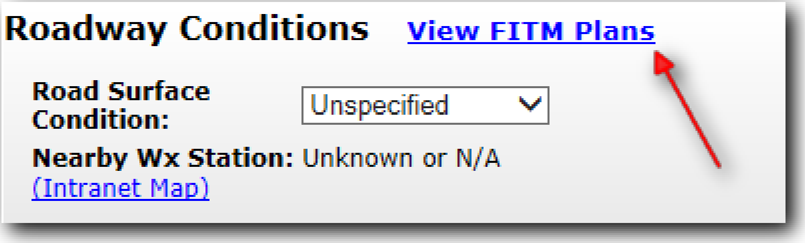


Figure 4-12. View FITM Plan (Details / PDF File)

4.2.3 View FITM Plans from Traffic Event

A user with the View FITM Plans functional right can view FITM plans from a traffic event that has a Roadway Conditions section (Incident, Weather, Special Event, or Planned Closure) by clicking on a new link, as shown in Figure 4-13.



Roadway Conditions View FITM Plans

Road Surface Condition: Unspecified

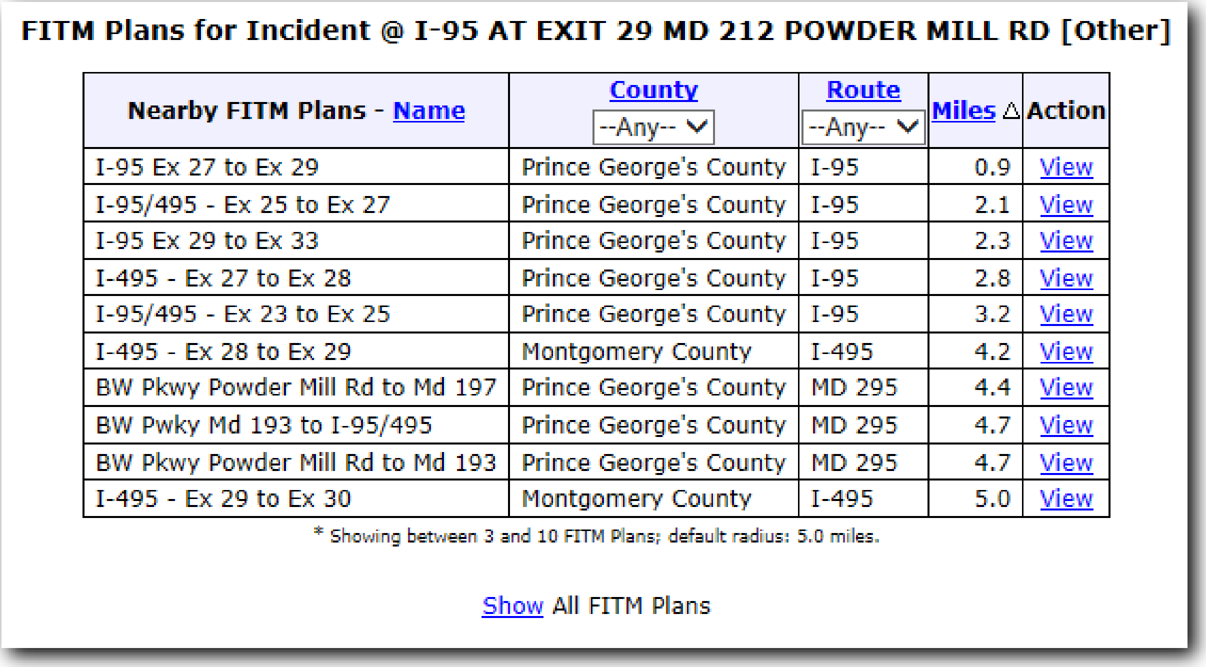
Nearby Wx Station: Unknown or N/A (Intranet Map)

Figure 4-13. FITM Plans Link (Event Details)

The link brings up the FITM Plans page, which appears differently depending on whether or not the traffic event has geographic (lat/long) coordinates:

4.2.3.1 FITM Plans for Traffic Event with Geographic Coordinates

If the traffic event has geographic coordinates, the initial FITM Plans list looks as shown in Figure 4-14.



FITM Plans for Incident @ I-95 AT EXIT 29 MD 212 POWDER MILL RD [Other]

Nearby FITM Plans - Name	County --Any--	Route --Any--	Miles △	Action
I-95 Ex 27 to Ex 29	Prince George's County	I-95	0.9	View
I-95/495 - Ex 25 to Ex 27	Prince George's County	I-95	2.1	View
I-95 Ex 29 to Ex 33	Prince George's County	I-95	2.3	View
I-495 - Ex 27 to Ex 28	Prince George's County	I-95	2.8	View
I-95/495 - Ex 23 to Ex 25	Prince George's County	I-95	3.2	View
I-495 - Ex 28 to Ex 29	Montgomery County	I-495	4.2	View
BW Pkwy Powder Mill Rd to Md 197	Prince George's County	MD 295	4.4	View
BW Pwky Md 193 to I-95/495	Prince George's County	MD 295	4.7	View
BW Pkwy Powder Mill Rd to Md 193	Prince George's County	MD 295	4.7	View
I-495 - Ex 29 to Ex 30	Montgomery County	I-495	5.0	View

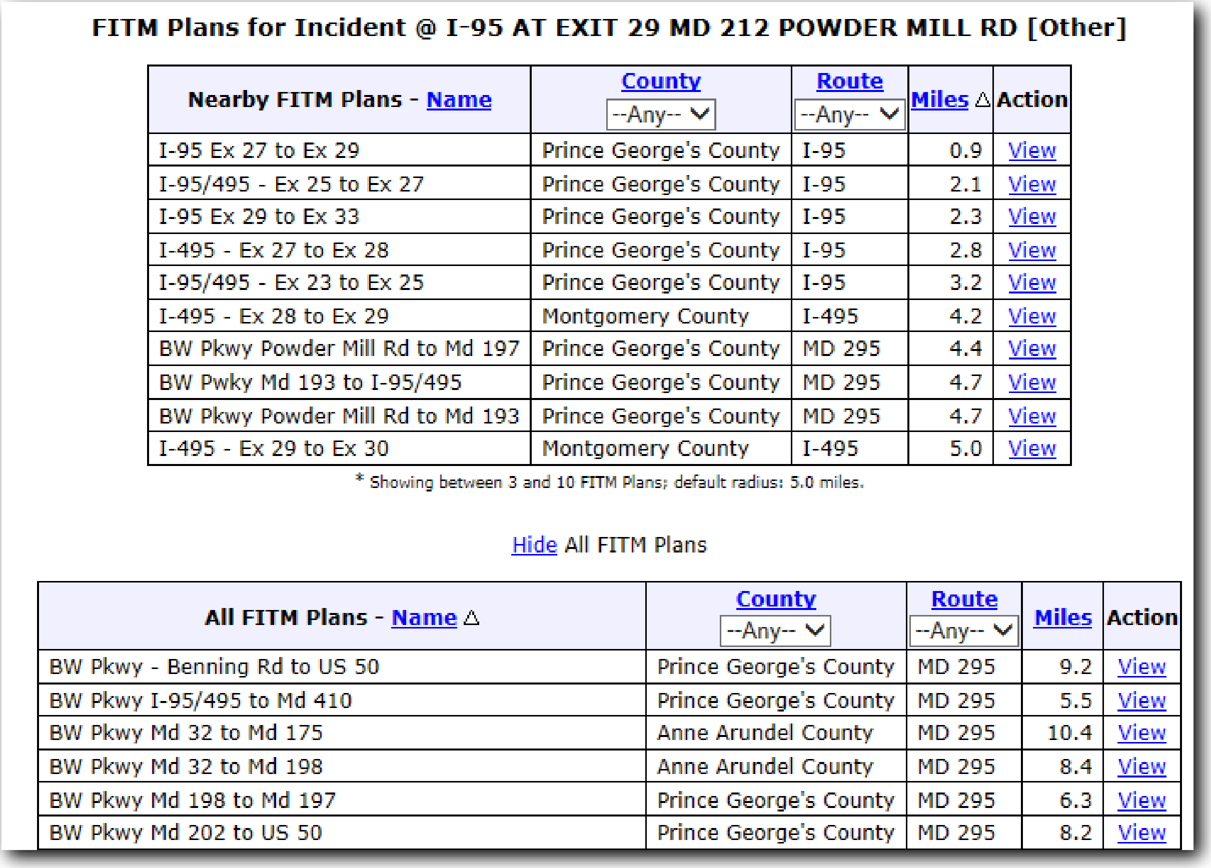
* Showing between 3 and 10 FITM Plans; default radius: 5.0 miles.

Show All FITM Plans

Figure 4-14. Nearby FITM Plans (Initial View)

The Nearby FITM Plans are initially shown, sorted by Miles (distance). The user can sort on Name, County, Route, or Miles. The user can also filter on County or Route. The text below the table describes the criteria for finding the nearby FITM plans.

When the screen is first displayed, the Nearby FITM Plans are shown, and the list of All FITM Plans is hidden. There is a Show link to show the list of all FITM plans, which if clicked on shows additional FITM plans, as shown in Figure 4-15.



FITM Plans for Incident @ I-95 AT EXIT 29 MD 212 POWDER MILL RD [Other]

Nearby FITM Plans - Name	County --Any--	Route --Any--	Miles △	Action
I-95 Ex 27 to Ex 29	Prince George's County	I-95	0.9	View
I-95/495 - Ex 25 to Ex 27	Prince George's County	I-95	2.1	View
I-95 Ex 29 to Ex 33	Prince George's County	I-95	2.3	View
I-495 - Ex 27 to Ex 28	Prince George's County	I-95	2.8	View
I-95/495 - Ex 23 to Ex 25	Prince George's County	I-95	3.2	View
I-495 - Ex 28 to Ex 29	Montgomery County	I-495	4.2	View
BW Pkwy Powder Mill Rd to Md 197	Prince George's County	MD 295	4.4	View
BW Pwky Md 193 to I-95/495	Prince George's County	MD 295	4.7	View
BW Pkwy Powder Mill Rd to Md 193	Prince George's County	MD 295	4.7	View
I-495 - Ex 29 to Ex 30	Montgomery County	I-495	5.0	View

* Showing between 3 and 10 FITM Plans; default radius: 5.0 miles.

Hide All FITM Plans

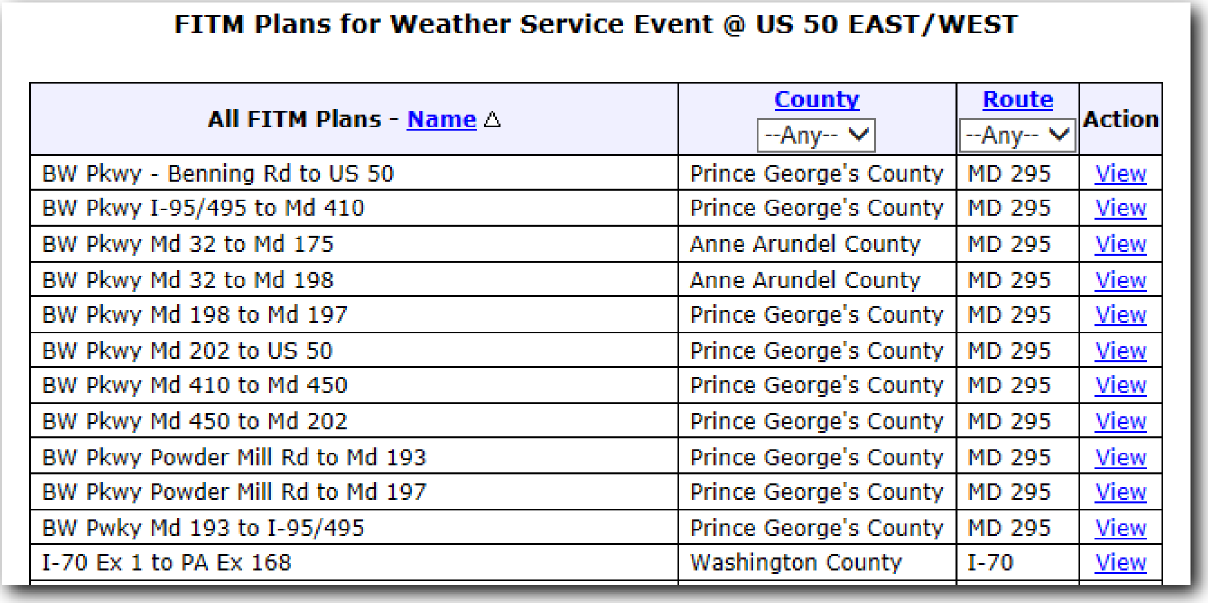
All FITM Plans - Name △	County --Any--	Route --Any--	Miles	Action
BW Pkwy - Benning Rd to US 50	Prince George's County	MD 295	9.2	View
BW Pkwy I-95/495 to Md 410	Prince George's County	MD 295	5.5	View
BW Pkwy Md 32 to Md 175	Anne Arundel County	MD 295	10.4	View
BW Pkwy Md 32 to Md 198	Anne Arundel County	MD 295	8.4	View
BW Pkwy Md 198 to Md 197	Prince George's County	MD 295	6.3	View
BW Pkwy Md 202 to US 50	Prince George's County	MD 295	8.2	View

Figure 4-15. Nearby and All FITM Plans

The list of All FITM Plans is initially sorted by Name. The user can sort on Name, County, Route, or Miles. The user can also filter on County or Route. The user can click on Hide to hide the All FITM Plans list.

4.2.3.2 FITM Plans for Traffic Event without Geographic Coordinates

If the traffic event does NOT have geographic coordinates, the All FITM Plans list is displayed, as shown in Figure 4-16.



FITM Plans for Weather Service Event @ US 50 EAST/WEST

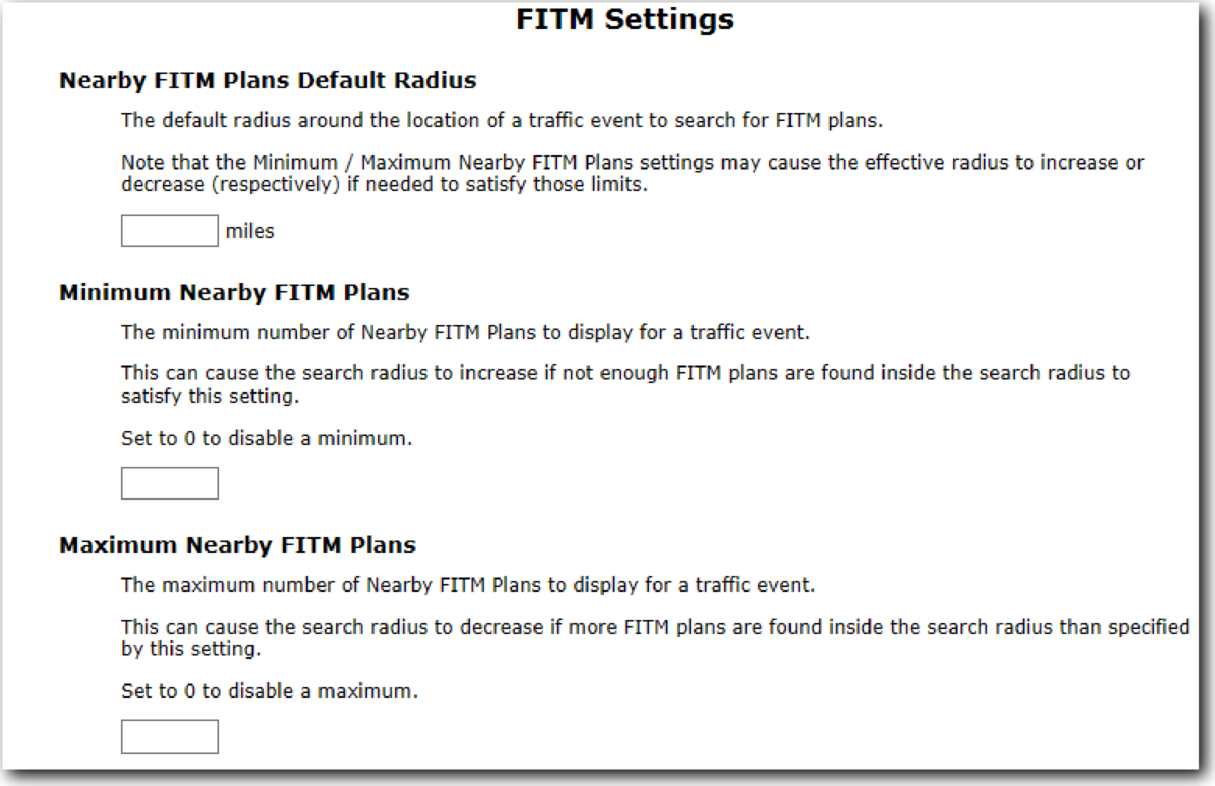
All FITM Plans - Name △	County --Any--	Route --Any--	Action
BW Pkwy - Benning Rd to US 50	Prince George's County	MD 295	View
BW Pkwy I-95/495 to Md 410	Prince George's County	MD 295	View
BW Pkwy Md 32 to Md 175	Anne Arundel County	MD 295	View
BW Pkwy Md 32 to Md 198	Anne Arundel County	MD 295	View
BW Pkwy Md 198 to Md 197	Prince George's County	MD 295	View
BW Pkwy Md 202 to US 50	Prince George's County	MD 295	View
BW Pkwy Md 410 to Md 450	Prince George's County	MD 295	View
BW Pkwy Md 450 to Md 202	Prince George's County	MD 295	View
BW Pkwy Powder Mill Rd to Md 193	Prince George's County	MD 295	View
BW Pkwy Powder Mill Rd to Md 197	Prince George's County	MD 295	View
BW Pwky Md 193 to I-95/495	Prince George's County	MD 295	View
I-70 Ex 1 to PA Ex 168	Washington County	I-70	View

Figure 4-16. FITM Plans for Event with No Coordinates

Note that the Nearby FITM Plans list and the Show / Hide link are NOT displayed.

4.2.4 FITM Configuration Settings

A user with the Configure System functional right can set the System Profile settings governing the behavior of the Nearby FITMs list for a traffic event. This is shown in Figure 4-17.



FITM Settings

Nearby FITM Plans Default Radius

The default radius around the location of a traffic event to search for FITM plans.

Note that the Minimum / Maximum Nearby FITM Plans settings may cause the effective radius to increase or decrease (respectively) if needed to satisfy those limits.

miles

Minimum Nearby FITM Plans

The minimum number of Nearby FITM Plans to display for a traffic event.

This can cause the search radius to increase if not enough FITM plans are found inside the search radius to satisfy this setting.

Set to 0 to disable a minimum.

Maximum Nearby FITM Plans

The maximum number of Nearby FITM Plans to display for a traffic event.

This can cause the search radius to decrease if more FITM plans are found inside the search radius than specified by this setting.

Set to 0 to disable a maximum.

Figure 4-17. FITM Configuration Settings

5 Acronyms/Glossary

Table 5-1defines acronyms and other terms used in this document.

Table 5-1. Acronyms & Glossary

Area of Responsibility	A geographic area that can be assigned to an operations center or monitor in order to define a boundary for information that the entity is responsible for/most interested in.
DMS	Dynamic Message Sign. An electronic sign used to display information to the traveling public.
Dynamic Message Sign	An electronic sign used to provide messages to motorists.
Functional right	A user right, granted to CHART users via Roles. Each operation on a device, including the ability to configure a device, view its sensitive information, and issue commands to the device are controlled by user rights. Users must possess the proper right to be able to perform these actions.
GIS	A Geographic Information System (GIS) is any system that captures, stores, analyzes, manages, and presents data that are linked to location
FITM Plan	Freeway Incident Traffic Management Plan. Describes a detour scenario when a specific portion of a main route is closed. Plans include a detour map and turn-by-turn instructions, and a list of affected traffic signals.
HAR	Highway Advisory Radio. A radio station used to broadcast programmable messages to motorists and other travelers regarding traffic and other delays.
Integrated Map	The mapping components that are part of the CHART user interface.
Intranet Map	The CHART Mapping application that is not integrated into the CHART user interface.
OpenLayers	Open source JavaScript mapping API utilized by the integrated map components in the CHART GUI.
Response Plan	A set of actions associated with a traffic event.
TTS	Text-to-Speech – a method for converted the written word to the spoken word.

6 Mapping To Requirements

Table 6-1shows how the requirements in the CHART R13 Requirements document map to design elements contained in this design.

Table 6-1. Mapping to Requirements

Tag	Requirement	Feature	Use Cases	Other Design Elements
SR1	ADMINISTER SYSTEMS AND EQUIPMENT		N/A	N/A
SR1.1	ADMINISTER CHART ORGANIZATIONS, LOCATIONS, AND USERS..		N/A	N/A
SR1.1.3	MAINTAIN CHART ROLES		N/A	N/A
SR1.1.3.2	The system shall allow the system administrator to remove a role.		N/A - unchanged for R13	Use Case Only
SR1.1.3.2.2	The system shall prevent removal of the role which matches the configured name of the specified official System Administrator role which has additional password requirements.	User Management	Delete Role	Use Case Only
SR1.1.3.5	The system shall allow a user with appropriate rights to add a role to the system.		N/A - unchanged for R13	N/A - unchanged for R13
SR1.1.3.5.1	The system shall allow the user to specify the name of the role.		N/A - unchanged for R13	N/A - unchanged for R13
SR1.1.3.5.1.1	The system shall allow the user to specify which role is designated the official System Administrator role, which has additional password requirements.	User Management	Specify User Management System Profile Settings	Use Case Only

Tag	Requirement	Feature	Use Cases	Other Design Elements
SR1.1.3.5.1.1.1	The system shall require the passwords of users who have the designated official System Administrator role to adhere to stricter password requirements with regard to password length (SR1.1.4.1.3.1) and expiration (SR1.4.1.3.8.4), as compared with users who do not have the designated official System Administrator role.	User Management	Set Password; Specify User Management System Profile Settings	OperationsCenterImpl.loginUser-private SD; UserManagerImpl.getUser SD; getUsersQuery/UserManagementDB.GetUsersQuery.handleResults SD
SR1.1.3.5.1.1.2	The system shall force the setting of the official System Administrator role to be the name of an existing role in the system or the empty string (which means that all users are considered normal users with respect to password length (SR1.1.4.1.3.1) and expiration (SR1.4.1.3.8.4)).	User Management	Specify User Management System Profile Settings	Use Case Only
SR1.1.4	MAINTAIN USERS		N/A	N/A
SR1.1.4.1	The system shall allow a user with the Configure Users right to add a user.	R11.1LevAPRs	N/A - unchanged for R13	Use Case Only
SR1.1.4.1.3	The system shall require the user to specify the new user's password.	R11.1LevAPRs	N/A - unchanged for R13	Use Case Only
SR1.1.4.1.3.1	The system shall require the user's password to be at least a minimum number of characters long.	User Management	Set Password	UserManagerImpl.validateNewPasswordLength SD
SR1.1.4.1.3.1.1	If any role set for the user is the designated official System Administrator role at the time the password is specified, the system shall require the user's password to be at least the configurable length defined for CHART System Administrators. (Policies as of 2013 require 11 characters.)	User Management	Set Password	UserManagerImpl.validateNewPasswordLength SD

Tag	Requirement	Feature	Use Cases	Other Design Elements
SR1.1.4.1.3.1.2	If the user is not set to have the designated official System Administrator role at the time the password is specified, the system shall require the user's password to be at least the configurable length defined for normal CHART users. (Policies as of 2013 require 8 characters.)	User Management	Set Password	UserManagerImpl.validateNewPasswordLength SD
SR1.1.4.1.3.1.3	If a proposed password is not long enough, the error message shall indicate the password must be at least N characters long, where N is the configured minimum number for the type of user for which the password is being set.	User Management	Set Password	UserManagerImpl.validateNewPasswordLength SD
SR1.1.4.1.3.1.4	The system shall constrain the settings for the minimum password lengths to be between 6 and 16 inclusive.	User Management	Specify User Management System Profile Settings	Use Case Only
SR1.1.4.1.3.2	The system shall require that the user's password to have a configured variety of character types.	User Management	Set Password	UserManagerImpl.validateNewPasswordDiversity SD
SR1.1.4.1.3.2.1	The system shall require that the user's password have at least a configurable number of letters of any case, uppercase or lowercase (A-Z and a-z). (Policies as of 2013 require at least 1 letter of any case.)	User Management	Set Password	UserManagerImpl.validateNewPasswordDiversity SD
SR1.1.4.1.3.2.2	The system shall require that the user's password have at least a configurable number of uppercase letters (A-Z). (Policies as of 2013 require at least 0 uppercase letters.)	User Management	Set Password	UserManagerImpl.validateNewPasswordDiversity SD

Tag	Requirement	Feature	Use Cases	Other Design Elements
SR1.1.4.1.3.2.3	The system shall require that the user's password have at least a configurable number of lowercase letters (a-z). (Policies as of 2013 require at least 0 lowercase letters.)	User Management	Set Password	UserManagerImpl.validateNewPasswordDiversity SD
SR1.1.4.1.3.2.4	The system shall require that the user's password have at least a configurable number of digits (0-9). (Policies as of 2013 require at least 1 digit.)	User Management	Set Password	UserManagerImpl.validateNewPasswordDiversity SD
SR1.1.4.1.3.2.5	The system shall require that the user's password have at least a configurable number of special characters (!@#$% etc). (Policies as of 2013 require at least 0 special characters.)	User Management	Set Password	UserManagerImpl.validateNewPasswordDiversity SD
SR1.1.4.1.3.2.5.1	The system shall allow a space as a special character within the user's password.	User Management	Set Password	UserManagerImpl.validateNewPassword SD
SR1.1.4.1.3.2.5.1.1	The system shall prohibit a space as the first or last character in the user's password.	User Management	Set Password	UserManagerImpl.validateNewPassword SD
SR1.1.4.1.3.2.5.1.1.1	If a proposed password contains a space at the beginning or end of the password, the error message will indicate the password cannot a space at the beginning or end of the password.	User Management	Set Password	UserManagerImpl.validateNewPassword SD
SR1.1.4.1.3.2.6	If a proposed password does not contain enough of a class of characters, the error message will indicate the password must contain at least N characters of the shorted class (for each class of character found to be shorted), where N is the configured minimum number.	User Management	Set Password	UserManagerImpl.validateNewPasswordDiversity SD

Tag	Requirement	Feature	Use Cases	Other Design Elements
SR1.1.4.1.3.2.7	The system shall constrain the settings for the minimum number for each class of character to zero, and ensure that configured minimum numbers for all classes of characters add up to no more than 16 (the largest-allowed minimum password length), counting either letters of any case OR the sum of uppercase and lowercase letters, whichever is larger (so as not to double-count letter requirements).	User Manage ment	Specify User Management System Profile Settings	Use Case Only
SR1.1.4.1.3.3	The system shall check the password against a dictionary which includes common words and proper names.	User Manage ment	Set Password	UserManagerImpl.validateNewPassword SD
SR1.1.4.1.3.3.1	The system shall reject the password if any maximal string of consecutive letters of any case matches any word in the dictionary of common words and proper names. (A "maximal" string of consecutive letters is defined as a complete string of letters delimited by non-letters, for example, the only maximal string of letters in "12mypassword!" is "mypassword", which will not be found in any dictionary, therefore that password is valid. The strings "my" and "password" are not maximal and therefore will not be checked as separate strings against the dictionary. However, in "my.password5", both "my" and "password" are maximal, so this password is not valid.)	User Manage ment	Set Password	UserManagerImpl.validateNewPassword SD

Tag	Requirement	Feature	Use Cases	Other Design Elements
SR1.1.4.1.3.3.1.1	If a proposed password contains a maximal string of letters found in the dictionary, the error message will indicate the password cannot contain an isolated word or name. (For security reasons, the system will not indicate the specific word(s) or name(s) found.)	User Manage ment	Set Password	UserManagerImpl.validateNewPassword SD
SR1.1.4.1.3.3.2	The system shall allow the requirement to use a dictionary to prohibit words and proper names in passwords to be disabled.	User Manage ment	Specify User Management System Profile Settings	UserManagerImpl.validateNewPassword SD
SR1.1.4.1.3.4	The system shall reject the password if it contains a string of a certain length of letters, digits, or special characters "in sequence".	User Manage ment	Set Password	UserManagerImpl.validateNewPasswordSequences SD
SR1.1.4.1.3.4.1	The system shall reject the password if it contains a string of a configurable length of letters of any case "in sequence", as defined by being contained within any of a set of configurable case-insensitive letter sequences. (A suggested length is 4 letters, and suggested prohibited letter sequences include "abcdefghijklmnopqrstuvwxyz", "zyxwvutsrqponmlkjihgfedcba", "qwertyuiop", "poiuytrewq", "asdfghjkl", "lkjhgfdsa", "zxcvbnm", "mnbvcxz". For instance, password "myPassmNop5" would be invalid because "mNop" is contained in "abcdefghijklmnopqrstuvwxyz".)	User Manage ment	Set Password	UserManagerImpl.validateNewPasswordSequences SD

Tag	Requirement	Feature	Use Cases	Other Design Elements
SR1.1.4.1.3.4.1.1	If a proposed password contains too many letters in sequence, the error message will indicate the password cannot contain N or more letters in sequence, where N is the number of letters prohibited. (For security reasons, the system will not indicate the specific sequence(s) of letters found or the length(s) of the sequence(s) found.)	User Management	Set Password	UserManagerImpl.validateNewPasswordSequences SD
SR1.1.4.1.3.4.2	The system shall reject the password if it contains a string of a configurable length of digits "in sequence", as defined by being contained within any of a set of configurable digit sequences. (A suggested length is 3 digits, and suggested prohibited digit sequences include "01234567890" and "09876543210". For instance, password "pass123321" would be invalid because "123" is contained in "01234567890" and "321" is contained in "09876543210". A length of 3 will catch "number pad" sequences such as "789456123".)	User Management	Set Password	UserManagerImpl.validateNewPasswordSequences SD
SR1.1.4.1.3.4.2.1	If a proposed password contains too many digits in sequence, the error message will indicate the password cannot contain N or more digits in sequence, where N is the number of digits prohibited. (For security reasons, the system will not indicate the specific sequence(s) of digits found or the length(s) of the sequence(s) found.)	User Management	Set Password	UserManagerImpl.validateNewPasswordSequences SD

Tag	Requirement	Feature	Use Cases	Other Design Elements
SR1.1.4.1.3.4.3	The system shall reject the password if it contains a string of a configurable length of special characters "in sequence", as defined by being contained within any of a set of configurable special character sequences. (A suggested length is 5 special characters, and suggested prohibited special character sequences include "!@#$%^&*()" and ")(*&^%$#@!". For instance, password "pass!@#$%" would be invalid because "!@#$%" is contained in "!@#$%^&*()".)	User Manage ment	Set Password	UserManagerImpl.validateNewPasswordSequences SD
SR1.1.4.1.3.4.3.1	If a proposed password contains too many special characters in sequence, the error message will indicate the password cannot contain N or more special characters in sequence, where N is the number of special characters prohibited. (For security reasons, the system will not indicate the specific sequence(s) of special characters found or the length(s) of the sequence(s) found.)	User Manage ment	Set Password	UserManagerImpl.validateNewPasswordSequences SD
SR1.1.4.1.3.4.4	The system shall constrain the settings for the prohibited sequence lengths of each class of character to a minimum of 2 (extremely restrictive) and a maximum of 10 (very lax), or to zero (which means the requirement is not enforced at all).	User Manage ment	Specify User Management Properties File Settings	Use Case Only

Tag	Requirement	Feature	Use Cases	Other Design Elements
SR1.1.4.1.3.5	The system will reject the password if it contains the same character a configurable number of times anywhere within the entire length of the password (not necessarily in a row). (A suggested number is 4 repeated characters. For instance, the password "a1a1a1a1" would be invalid because it contains 4 "a" and 4 "1" characters.)	User Management	Set Password	UserManagerImpl.validateNewPasswordRepeatedChars SD
SR1.1.4.1.3.5.1	If a proposed password contains too many repeated characters, the error message will indicate the password cannot contain the same character N or more times (where N is the configurable number). (For security reasons, the system will not indicate the number of characters that had too much repetition, the number of times the character(s) were repeated, or identify the repeated character(s).)	User Management	Set Password	UserManagerImpl.validateNewPasswordRepeatedChars SD
SR1.1.4.1.3.5.2	The system shall constrain the setting for the prohibited number of repeated characters to a minimum of 2 (extremely restrictive) and a maximum of 10 (very lax), or to zero (which means the requirement is not enforced at all).	User Management	Specify User Management Properties File Settings	Use Case Only
SR1.1.4.1.3.6	When a user is creating a password, the system shall provide help text describing all the password rules currently in effect to aid in creating a valid password.	User Management	Set Password	Use Case Only
SR1.1.4.1.6	The system shall allow the user to specify whether the new user's account is enabled or disabled.	User Management	Add User Account	UserManagementModule CD

Tag	Requirement	Feature	Use Cases	Other Design Elements
SR1.1.4.1.6.1	When a new user account is added, the default state of the new user's account shall be enabled.	User Management	Add User Account	Use Case Only
SR1.1.4.4	The system shall allow the system administrator to set the user password.		Reset User's Password; Add User Account	UserManagerImpl.resetOtherUsersPassword SD
SR1.1.4.4.1	When administratively setting (resetting) another user's password, all requirements for setting a password for a brand new user under requirement SR1.1.4.1.3 shall pertain.	User Management	Reset User's Password	UserManagerImpl.resetOtherUsersPassword SD; UserManagerImpl.validateNewPassword SD
SR1.1.4.9	The system shall allow a user with the Configure Users right or the View User Configuration right to view the users defined in the system.	R11.1LevAPRs	N/A - unchanged for R13	Use Case Only
SR1.1.4.9.1	The system shall allow the following information to be viewed for each user: User Name, Default Center, Other Centers capability, Selected Other Centers, account Enabled/Disabled status, Last Login time stamp, and Last Login Center.	R11.1LevAPRs, User Management	View User Accounts	Use Case Only
SR1.1.4.9.2	The system shall allow the user to sort the list using the data in the following columns: User Name, Default Center, Other Centers capability, Selected Other Centers, account Enabled/Disabled status, Last Login time stamp, and Last Login Center.	R11.1LevAPRs, User Management	View User Accounts	Use Case Only

Tag	Requirement	Feature	Use Cases	Other Design Elements
SR1.1.4.9.3	The system shall allow the user to filter the list using data in the following columns: User Name, Default Center, Other Centers capability, Selected Other Centers, account Enabled/Disabled status, Last Login time stamp, and Last Login Center.	R11.1LevAPRs, User Management	View User Accounts	Use Case Only
SR1.1.4.9.4	The system shall allow the user to choose to show or hide the following columns of data: Default Center, Other Centers capability, Selected Other Centers, account Enabled/Disabled status, Last Login time stamp, and Last Login Center.	R11.1LevAPRs, User Management	View User Accounts	Use Case Only
SR1.1.4.10	The system shall allow a system administrator to enable a user's account.	User Management	Enable User Account	UserManagerImpl.setAcctDisabledStatus SD
SR1.1.4.11	The system shall allow a system administrator to disable a user's account.	User Management	Disable User Account	UserManagerImpl.setAcctDisabledStatus SD
SR1.1.4.11.1	If a user is logged in when his/her account becomes disabled, that user will automatically be logged out.	User Management	Disable User Account	UserManagerImpl.setAcctDisabledStatus SD
SR1.1.4.12	The system shall automatically disable any account not used for a configurable number of days.	User Management	Disable User Account	AccountDisablerTimerTask.run SD; UserManagerImpl.setAcctDisabledStatus SD
SR1.1.4.12.1	The system shall constrain the setting for the number of days an account must be inactive before it is disabled to a minimum of 7 (extremely restrictive) and a maximum of 365 (very lax), or to zero (which means the requirement is not enforced at all).	User Management	Specify User Management Properties File Settings	Use Case Only
SR1.4	MANAGE CHART CONTROL		N/A	N/A
SR1.4.1	CONTROL LOGIN		N/A	N/A

Tag	Requirement	Feature	Use Cases	Other Design Elements
SR1.4.1.1	The system shall require a user to provide a user name and password in order to log in.	R11.1LevAPRs	N/A - unchanged for R13	Use Case Only
SR1.4.1.1.1	The system will provide a usage warning to the user on the login screen, using SHA-provided text. (The text is intended to advise users that access is restricted to authorized users only, that unauthorized use is prohibited and subject to prosecution, that user activity on the system is monitored, that data created becomes property of the State of Maryland, etc.)	User Management	Log In	Use Case Only
SR1.4.1.1.2	If the user's account is disabled, after the user has entered the user ID and current password correctly, the system will prevent the user from logging on with a message to the effect that the account has been disabled.	User Management	Log In	OperationsCenterImpl.loginUser-private SD
SR1.4.1.3	The system shall attempt to log a user into the selected operations center using the user name and password provided.	R11.1LevAPRs	N/A - unchanged for R13	Use Case Only
SR1.4.1.3.2	The system shall temporarily lock a user's account for a configurable number of minutes after a configurable number of consecutive failed login attempts within a configurable number of minutes. (Do not confuse this temporary "locking" with "disabling" of accounts, which is permanent (until reversed by a CHART ATMS administrator).)	User Management	Temporarily Lock User Account	OperationsCenterImpl.loginUser-private SD

Tag	Requirement	Feature	Use Cases	Other Design Elements
SR1.4.1.3.2.1	When a user's account is locked due to consecutive failed login attempts, the system shall indicate this to the user, together with the time at which a login attempt will again be submitted and processed.	User Manage ment	Log In	OperationsCenterImpl.loginUser-private SD
SR1.4.1.3.2.2	When a user's account is locked due to consecutive failed login attempts, the system shall automatically unlock the account after the configured delay. (No user or administrator unlock action is necessary.)	User Manage ment	Unlock User Account	OperationsCenterImpl.loginUser-private SD
SR1.4.1.3.2.2.1	If an administrator resets the password of a user whose account has been locked, the user's account shall be immediately unlocked. (Although no administrator action is necessary, this action will restore access if access is required immediately -- or if the user truly has forgotten the correct password.)	User Manage ment	Reset User's Password	OperationsCenterImpl.loginUser-private SD
SR1.4.1.3.2.3	The system shall constrain the setting for the number of consecutive failed login attempts to a minimum of 3 (restrictive) and a maximum of 20 (very lax), or to zero (which means the requirement is not enforced at all).	User Manage ment	Specify User Management Properties File Settings	Use Case Only

Tag	Requirement	Feature	Use Cases	Other Design Elements
SR1.4.1.3.2.4	The system shall constrain the setting for the number of minutes over which the consecutive failed login attempts must occur to cause a lock to a minimum of 3 (loose security) and no maximum (tighter security), or to zero (which means the failed login attempts can be indefinitely far apart and still cause a lock, tightest security).	User Management	Specify User Management Properties File Settings	Use Case Only
SR1.4.1.3.2.5	The system shall constrain the setting for the number of minutes the account will be locked after the consecutive failed login attempts to a minimum of 3 (minimal security, minimal user impact) and a maximum of 60 (tight security, severe user impact) , or to zero (which means the requirement is not enforced at all).	User Management	Specify User Management Properties File Settings	Use Case Only
SR1.4.1.3.8	If the user login is not rejected, the system shall log them into the requested operations center.	R11.1LevAPRs	N/A - unchanged for R13	Use Case Only
SR1.4.1.3.8.2	The system shall display a data disclaimer using SHA-provided text to the user upon successful login. (The intent of the disclaimer is to warn users that the data may be suspect for a variety of reasons and that the data is provided "as is" without warranty.)	User Management	N/A - unchanged for R13	N/A - unchanged for R13
SR1.4.1.3.8.2.1	The system shall require the user to acknowledge the data disclaimer prior to allowing the user access to the system.	User Management	N/A - unchanged for R13	N/A - unchanged for R13

Tag	Requirement	Feature	Use Cases	Other Design Elements
SR1.4.1.3.8.3	Upon successful login, the system shall display to the user the last time (prior to the current login) that user successfully logged in and the last time that user successfully logged out. (Note that if a user session is forced out, timed out, or otherwise aborted, the last successful logout may be further back in the past than the last successful login.)	User Management	Log In	OperationsCenterImpl.loginUser-private SD
SR1.4.1.3.8.4	If the user's password has expired, the system shall force the user to change his/her password immediately, prior to allowing the user access to the system.	User Management	Log in; Set Own Password	OperationsCenterImpl.loginUser-private SD
SR1.4.1.3.8.4.1	If the user has the designated official System Administrator role at the time of login, the user's password shall be deemed to have expired if the password has not been changed in a configurable number of days specified for official CHART System Administrators. (Policies as of 2013 require System Administrator passwords to expire after 30 days.)	User Management	Log in; Set Own Password	OperationsCenterImpl.loginUser-private SD
SR1.4.1.3.8.4.2	If the user does not have the designated official System Administrator role at the time of login, the user's password shall be deemed to have expired if the password has not been changed in a configurable number of days specified for normal CHART users. (Policies as of 2013 require normal user passwords to expire after 45 days.)	User Management	Log in; Set Own Password	OperationsCenterImpl.loginUser-private SD

Tag	Requirement	Feature	Use Cases	Other Design Elements
SR1.4.1.3.8.4.3	In lieu of immediately changing his/her expired password, the system shall allow the user to abort the login and be immediately logged out of the CHART ATMS instead.	User Management	Log in; Set Own Password	OperationsCenterImpl.loginUser-private SD
SR1.4.1.3.8.4.4	The system shall constrain the setting for the password expiration times to be a minimum of 7 days (extremely high user impact) and a maximum of 365 (low user impact, minimal security benefit), or to zero (passwords never expire).	User Management	Specify User Management Properties File Settings	Use Case Only
SR1.4.1.3.8.6	If the user's current password has been set by a CHART administrator, the system shall force the user to change his/her password immediately, prior to allowing the user access to the system.	User Management	Log In	OperationsCenterImpl.loginUser-private SD
SR1.4.1.3.8.6.1	In lieu of immediately changing his/her administratively-set password, the system shall allow the user to abort the login and be immediately logged out of the CHART ATMS instead.	User Management	Log In	Use Case Only
SR1.4.1.10	The system shall allow a user to change his/her own password, in accordance with this requirement's subrequirements and SR1.1.4.1.3 and all its subrequirements.	User Management	N/A - unchanged for R13	N/A - unchanged for R13
SR1.4.1.10.1	The system shall prohibit the user from changing his/her own password in a minimal way.	User Management	Change Password	UserManagerImpl.validateNewPasswordChangedEnough
SR1.4.1.10.1.1	The system shall prevent the user from changing his/her own password only by adding a single character anywhere within the current password.	User Management	Change Password	UserManagerImpl.validateNewPasswordChangedEnough

Tag	Requirement	Feature	Use Cases	Other Design Elements
SR1.4.1.10.1.1.1	The system shall allow the requirement which prohibits changing a password by adding a single character to be disabled.	User Management	Specify User Management Properties File Settings	UserManagerImpl.validateNewPasswordChangedEnough
SR1.4.1.10.1.2	The system shall prevent the user from changing her/her own password only by changing a single character in the current password.	User Management	Change Password	UserManagerImpl.validateNewPasswordChangedEnough
SR1.4.1.10.1.2.1	The system shall allow the requirement which prohibits changing a password by changing a single character to be disabled.	User Management	Specify User Management Properties File Settings	UserManagerImpl.validateNewPasswordChangedEnough
SR1.4.1.10.1.3	The system shall prevent the user from changing her/her own password only by deleting a single character in the current password.	User Management	Change Password	UserManagerImpl.validateNewPasswordChangedEnough
SR1.4.1.10.1.3.1	The system shall allow the requirement which prohibits changing a password by deleting a single character to be disabled.	User Management	Specify User Management Properties File Settings	UserManagerImpl.validateNewPasswordChangedEnough
SR1.4.1.10.2	The system shall prohibit the user from re-using any of a configurable number of his/her most recently used passwords (counting the current password as the first most recently used password). (Note that password history starts with deployment of R13; there is no history to check against prior to R13.)	User Management	Change Password	UserManagerImpl.validateNewPasswordNotReusedSD
SR1.4.1.10.2.1	The system shall constrain the setting for the history of previous passwords saved and checked for re-use to a minimum of zero (which disables the requirement) and a maximum of 50 (about four years' worth if changed every month).	User Management	Specify User Management Properties File Settings	Use Case Only

Tag	Requirement	Feature	Use Cases	Other Design Elements
SR1.4.1.10.3	The system shall prevent the user from changing her/her own password more than a configurable number of times within a configurable number of days. (Policies as of 2013 allow for no more than 1 password change within 2 days.)	User Management	Change Password	UserManagerImpl.changeOwnPassword SD
SR1.4.1.10.3.1	If an administrator resets a user's password, the system shall force the user to change his/her own password upon next login, in accordance with requirement SR1.4.1.3.8.4, even if the user has exceeded the allowed number of password changes within the current time period.	User Management	Change Password	UserManagerImpl.changeOwnPassword SD
SR1.4.1.10.3.2	The system shall constrain the setting for the time period over which password changes are restricted to a minimum of zero (which disables the requirement) and a maximum of one day less than the lower of the two classes of password expiration times as described in requirement SR1.4.1.3.8.4. (For example, if administrator passwords are set to expire every 14 days, users cannot be restricted to changing their passwords only once every 14 days: they must be able to change passwords after 13 days at most, otherwise users could be prohibited from changing their own password even though it has expired.)	User Management	Specify User Management Properties File Settings	Use Case Only

Tag	Requirement	Feature	Use Cases	Other Design Elements
SR1.4.1.10.3.3	The system shall constrain the setting for the number of times users can change their password within a certain time period to a minimum of zero (which disables the requirement) and a maximum of 5 (by which point it provides no substantive security benefit).	User Management	Specify User Management Properties File Settings	Use Case Only
SR4	MANAGE EVENTS		N/A	N/A (Heading)
SR4.2	OPEN EVENT		N/A	N/A (Heading)
SR4.2.3	DEPLOY RESOURCES. The system shall allow the user to view the pre-defined decision support plans to suggest the course of action and notifications, and execute the selected (or modified) course of action. The ability to record the deploying of the resources only applies to user generated events – not External Events. *		N/A	N/A (Included for context)
SR4.2.3.2	EVALUATE EVENT RESPONSE RECOMMENDATIONS. The system shall display the most appropriate corresponding recommended response plan from the pre-defined decision support plans, based on the event type, conditions, day of week and time of day (e.g., to determine closest open maintenance shop), location, and area of responsibility.		N/A	N/A (Included for context)
SR4.2.3.2.4	The system shall display the recommended FITM(s), alternate routes, and evacuation routes.		N/A (heading)	N/A (Heading)
SR4.2.3.2.4.1	View FITM Plans	FITMs	N/A (heading)	N/A (Heading)

Tag	Requirement	Feature	Use Cases	Other Design Elements
SR4.2.3.2.4.1.1	The system shall allow a user with the View FITM Plans right to view the All FITM Plans list from outside the context of a traffic event.	FITMs	View All FITM Plans	Prototype / HMI, FITMReqHdlr.getFITMPlans1and2 SD
SR4.2.3.2.4.1.2	The system shall allow a user with the View FITM Plans right to view FITM plans from the context of a traffic event of any type that supports roadway conditions (i.e., Incident, Planned Closure, Special Event, or Weather Service Event).	FITMs	View Nearby FITM Plans	Prototype / HMI only
SR4.2.3.2.4.1.2.1	The system shall show a list of Nearby FITM Plans if the traffic event has geographic (lat/long) coordinates.	FITMs	View Nearby FITM Plans	Prototype / HMI, FITMReqHdlr.getFITMPlans1and2 SD, FITMReqHdlr.getFITMPlans3 SD
SR4.2.3.2.4.1.2.1.1	The Nearby FITM Plans list shall include FITM plans located within a default search radius from the location of the event.	FITMs	View Nearby FITM Plans	FITMDynListDelegateSupporter.getNearbyFITMSubjects SD
SR4.2.3.2.4.1.2.1.1.1	The system shall allow a user with the Configure System right to specify the system-wide default search radius for Nearby FITM plans.	FITMs	Configure FITM Search Criteria	Prototype / HMI, GUIDataClassesR13 CD
SR4.2.3.2.4.1.2.1.2	The Nearby FITM Plans list shall include a minimum number of FITM plans.	FITMs	View Nearby FITM Plans	FITMDynListDelegateSupporter.getNearbyFITMSubjects SD
SR4.2.3.2.4.1.2.1.2.1	The minimum number of Nearby FITM Plans shall override the default search radius, if necessary. (In other words, the effective search radius will increase until the minimum number of FITM Plans are found).	FITMs	View Nearby FITM Plans	FITMDynListDelegateSupporter.getNearbyFITMSubjects SD

Tag	Requirement	Feature	Use Cases	Other Design Elements
SR4.2.3.2.4.1.2.1.2.2	The system shall allow a user with the Configure System right to specify the system-wide minimum number of Nearby FITM plans to display.	FITMs	Configure FITM Search Criteria	Prototype / HMI, GUIDataClassesR13 CD
SR4.2.3.2.4.1.2.1.3	The system shall limit the number of FITM plans in the Nearby FITM Plans list.	FITMs	View Nearby FITM Plans	FITMDynListDelegateSupporter.getNearbyFITMSubjects SD
SR4.2.3.2.4.1.2.1.3.1	The maximum number of Nearby FITM Plans shall override the initial search radius. (In other words, the effective search radius will decrease if the maximum number of FITM plans are found closer to the event than the initial search radius).	FITMs	View Nearby FITM Plans	FITMDynListDelegateSupporter.getNearbyFITMSubjects SD
SR4.2.3.2.4.1.2.1.3.2	The system shall allow a user with the Configure System right to specify the system-wide maximum number of Nearby FITM Plans to display.	FITMs	Configure FITM Search Criteria	Prototype / HMI, GUIDataClassesR13 CD
SR4.2.3.2.4.1.2.1.4	The system shall display the search criteria that were used to find the Nearby FITM Plans.	FITMs	View Nearby FITM Plans	Prototype / HMI only
SR4.2.3.2.4.1.2.1.5	The Nearby FITM Plans list shall show the name, county, route, and distance for each FITM plan, if available.	FITMs	View Nearby FITM Plans	Prototype / HMI, FITMServletClasses CD
SR4.2.3.2.4.1.2.1.6	The Nearby FITM Plans list shall allow the user to filter by county or route.	FITMs	View Nearby FITM Plans	Prototype / HMI, FITMServletClasses CD
SR4.2.3.2.4.1.2.1.7	The system shall allow the user to sort the Nearby FITM Plans list by name, county, route, or distance.	FITMs	View Nearby FITM Plans	Prototype / HMI, FITMServletClasses CD
SR4.2.3.2.4.1.2.1.7.1	The Nearby FITM Plans list shall be initially sorted by distance.	FITMs	View Nearby FITM Plans	Prototype / HMI
SR4.2.3.2.4.1.2.2	The system shall allow the user to view a list of All FITM Plans from the context of a traffic event.	FITMs	View All FITM Plans	Prototype / HMI, FITMServletClasses CD, FITMReqHdlr.getFITMPlans1and2 SD

Tag	Requirement	Feature	Use Cases	Other Design Elements
SR4.2.3.2.4.1.2.2.1	The All FITM Plans list shall be hidden by default if the Nearby FITM Plans are displayed.	FITMs	View All FITM Plans	Prototype / HMI only
SR4.2.3.2.4.1.2.2.2	The system shall allow the user to show or hide the All FITM Plans list, if Nearby FITM Plans are displayed.	FITMs	View All FITM Plans	Prototype / HMI only
SR4.2.3.2.4.1.2.2.3	The All FITM Plans list shall show the Distance (air miles) between the traffic event and the FITM plan, if the traffic event has geographic (lat/long) coordinates.	FITMs	View All FITM Plans	Prototype / HMI, FITMServletClasses CD
SR4.2.3.2.4.1.2.2.3.1	The system shall allow the user to sort the All FITM Plans list by Distance.	FITMs	View All FITM Plans	Prototype / HMI, FITMServletClasses CD
SR4.2.3.2.4.1.2.3	The system shall log an entry in the traffic event history log when a user views a FITM plan PDF file from the context of a traffic event.	FITMs	View FITM Plan File	Use Case Only
SR4.2.3.2.4.1.3	The system shall allow a user viewing the All FITM Plans list to view, sort, and/or filter the FITM plans in the list. (This applies to viewing the list from both contexts: from within the context of a traffic event, or from outside the context of a traffic event).	FITMs	View All FITM Plans	Prototype / HMI, FITMServletClasses CD
SR4.2.3.2.4.1.3.1	The All FITM Plans list shall show the name, county, and route for each FITM plan, if available.	FITMs	View All FITM Plans	Prototype / HMI, FITMServletClasses CD
SR4.2.3.2.4.1.3.2	The system shall allow the user to sort the All FITM Plans list by name, county, or route.	FITMs	View All FITM Plans	Prototype / HMI only
SR4.2.3.2.4.1.3.2.1	The system shall by default sort the All FITM Plans list by name.	FITMs	View All FITM Plans	Prototype / HMI only
SR4.2.3.2.4.1.3.3	The system shall allow the user to filter the All FITM Plans list by county or route.	FITMs	View All FITM Plans	Prototype / HMI only

Tag	Requirement	Feature	Use Cases	Other Design Elements
SR4.2.3.2.4.1.4	The system shall allow a user viewing a list of FITM plans to view the PDF file for a FITM plan.	FITMs	View FITM Plan File	Prototype / HMI, ServletClassesR13 CD

7 Use Case Diagrams

The use case diagrams depict new functionality for CHART ATMS R13 and also identify existing features that will be enhanced. The use case diagrams exist in the Enterprise Architect design tool in the chartdesign project, under the CHART-ATMS-R13 folder.

7.1 Security Policy Enhancements Feature

7.1.1 Security Policy Enhancements

Figure 7-1 shows use cases related to the Security Policy Enhancements feature for R13.

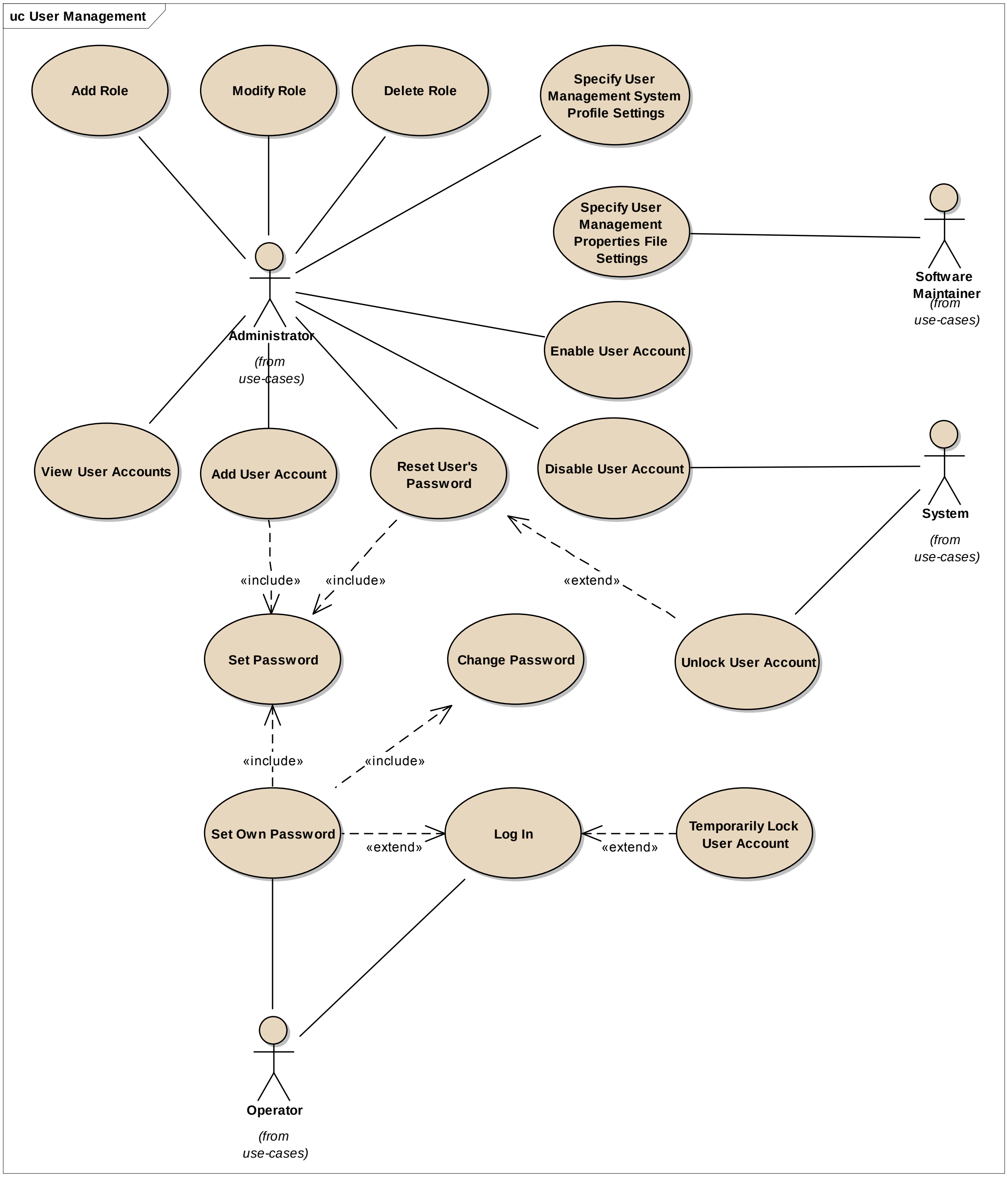


Figure 7-1 Security Policy Enhancements Use Cases

7.2 FITM Plans Feature

7.2.1 FITM Plans

Figure 7-2 shows use cases related to FITM Plans.

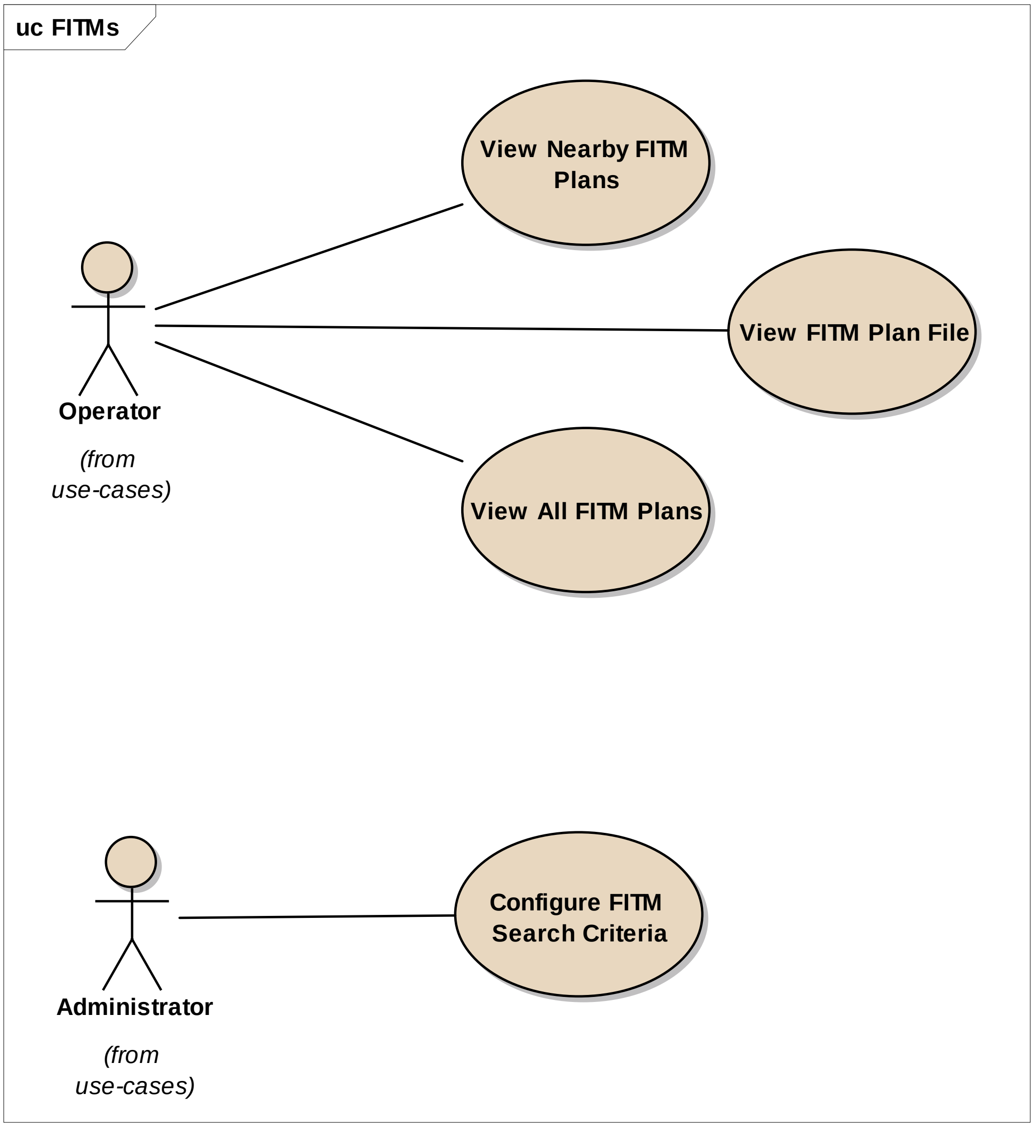


Figure 7-2. FITMs Use Cases

8 System Interfaces Design (IDL)

For convenient viewing, new and modified IDL designs are included in a separate document for viewing with a browser. Open the file `index.htm`. See the example in Figure 8-1 for where to find links to the classes → IDLInterfaces diagrams.

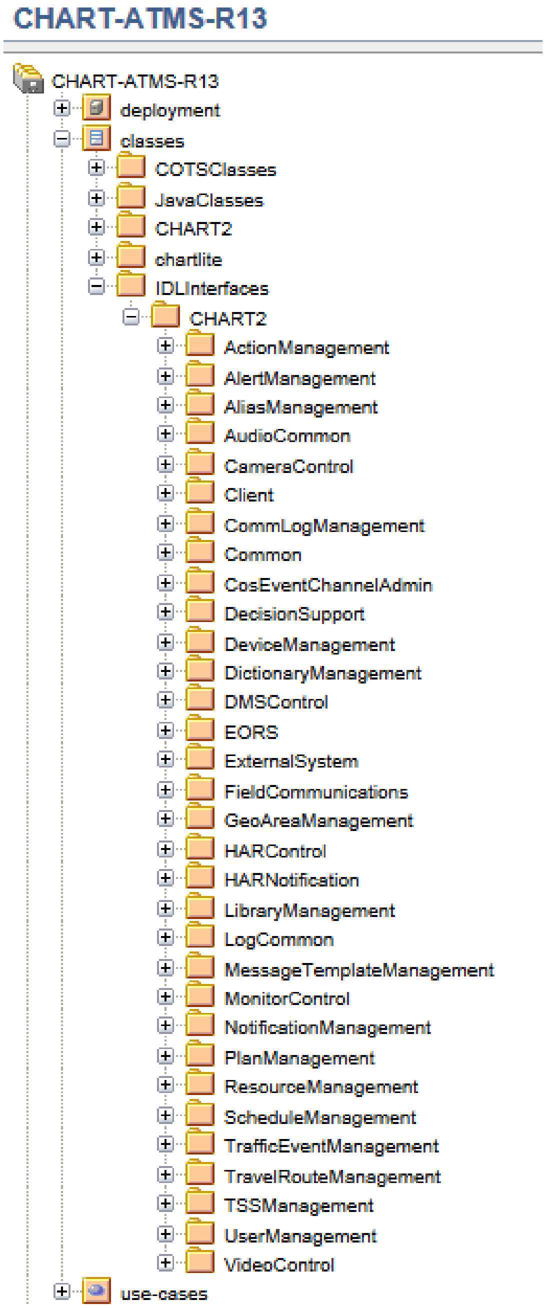


CHART-ATMS-R13

- CHART-ATMS-R13
  - deployment
  - classes
    - COTSClasses
    - JavaClasses
    - CHART2
    - chartlite
    - IDLInterfaces
      - CHART2
        - ActionManagement
        - AlertManagement
        - AliasManagement
        - AudioCommon
        - CameraControl
        - Client
        - CommLogManagement
        - Common
        - CosEventChannelAdmin
        - DecisionSupport
        - DeviceManagement
        - DictionaryManagement
        - DMSControl
        - EORS
        - ExternalSystem
        - FieldCommunications
        - GeoAreaManagement
        - HARControl
        - HARNotification
        - LibraryManagement
        - LogCommon
        - MessageTemplateManagement
        - MonitorControl
        - NotificationManagement
        - PlanManagement
        - ResourceManagement
        - ScheduleManagement
        - TrafficEventManagement
        - TravelRouteManagement
        - TSSManagement
        - UserManagement
        - VideoControl
  - use-cases

Figure 8-1. Where to Find IDL Interfaces Classes in HTML Design

IDL Class diagrams relevant for R13 are contained in ResourceManagement and UserManagement folders listed in the figure. The class diagrams are:

```
IDLInterfaces/ResourceManagement/ResourceManagementIDLClasses CD
IDLInterfaces/UserManagement/UserManagementIDLClasses CD
```

9 Package Designs

For convenient viewing, new and modified package designs are included in a separate document for viewing with a browser. Open the file `index.htm`. See Figure 9-1 for where to find links to the classes → CHART2 diagrams and classes → chartlite diagrams.

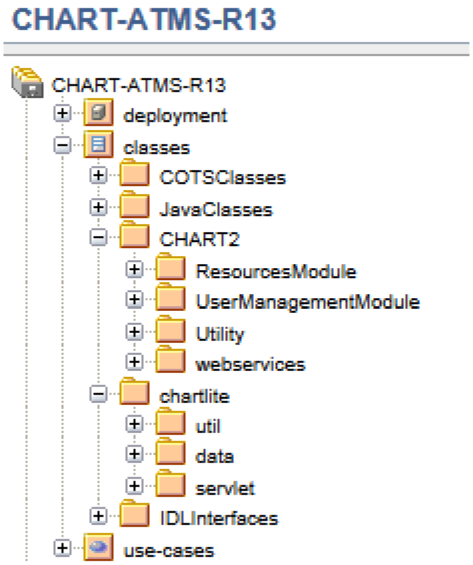


Figure 9-1. Where to Find CHART2 Classes in HTML Design

Relevant class diagrams for R13 are:

```
CHART2/ResourcesModule/ResourcesModule CD
CHART2/UserManagementModule/UserManagementModule CD
CHART2/Utility/Utility CD
chartlite/data/GUIDataClassesR13 CD
chartlite/data/fitm/FITMClasses CD
chartlite/servlet/ServletClassesR13 CD
chartlite/servlet/fitm/FITMServletClasses CD
```

Relevant sequence diagrams for R13 are:

`Under CHART2/ResourcesModule/OperationsCenterImpl/ --`
`OperationsCenterImpl.loginUser-private SD`

`Under CHART2/UserManagementModule/AccountDisablerTimerTask/ --`
`AccountDisablerTimerTask.run SD`

`Under CHART2/UserManagementModule/UserManagementDB/ --`
`UserManagementDB.addLoginFailure SD`
`UserManagementDB.setUserPassword SD`
`getUsersQuery/UserManagementDB.GetUsersQuery.handleResults SD`

Under CHART2/UserManagementModule/UserManagerImpl/ --
UserManagerImpl.breakDownPasswordByCharType SD
UserManagerImpl.changeOwnPassword SD
UserManagerImpl.getUser SD
UserManagerImpl.resetOtherUsersPassword SD
UserManagerImpl.setAcctDisabledStatus SD
UserManagerImpl.validateNewPassword SD
UserManagerImpl.validateNewPasswordChangedEnough SD
UserManagerImpl.validateNewPasswordDiversity SD
UserManagerImpl.validateNewPasswordLength SD
UserManagerImpl.validateNewPasswordNotReused SD
UserManagerImpl.validateNewPasswordRepeatedChars SD
UserManagerImpl.validateNewPasswordSequences SD

Under chartlite/data/fitm/DiscoverFITMPlansCommand/ --
UserManagerImpl.DiscoverFITMPlansCommand.execute SD

Under chartlite/servlet/fitm/FITMDynListDelegateSupporter/ --
FITMDynListDelegateSupporter.getNearbyFITMSubjects SD

Under chartlite/servlet/fitm/FITMDynListDelegateSupporter/ --
FITMDynListDelegateSupporter.getSubjectsToDisplay SD

Under chartlite/servlet/fitm/FITMReqHdlr/ --
FITMReqHdlr.getFITMPlans1and2 SD
FITMReqHdlr.getFITMPlans3 SD